serie de matemática monografía no. 25

ARITMETICA ELEMENTAL

Secretaría General de la
Organización de los Estados Americanos
Programa Regional de Desarrollo Científico y Tecnológico

ARITMETICA ELEMENTAL

por

Enzo R. Gentile
Universidad de Buenos Aires y
Consejo Nacional de Investigaciones
Científicas y Técnicas
Buenos Aires, ARGENTINA

Secretaría General de la
Organización de los Estados Americanos
Programa Regional de Desarrollo Científico y Tecnológico
Washington, D.C. - 1985

Esta monografía ha sido preparada para su publicación en el Departamento de Asuntos Científicos y Tecnológicos de la Secretaría General de la Organización de los Estados Americanos.

Editora: Eva V. Chesneau

Asesor Técnico: Ing. Andrés Valeiras
División de Ciencias Básicas
Departamento de Asuntos Científicos y Tecnológicos
Secretaría General de la
Organización de los Estados Americanos
Washington, D.C., EE.UU.

A los lectores

El programa de monografías científicas es un aspecto de la vasta labor de la Organización de los Estados Americanos, a cargo del Departamento de Asuntos Científicos y Tecnológicos de la Secretaría General de dicha Organización, a cuyo financiamiento contribuye en forma importante el Programa Regional de Desarrollo Científico y Tecnológico.

Concebido por los Jefes de Estado Americanos en su Reunión celebrada en Punta del Este, Uruguay, en 1967, y cristalizado en las deliberaciones y mandatos de la Quinta Reunión del Consejo Interamericano Cultural, llevada a cabo en Maracay, Venezuela, en 1968, el Programa Regional de Desarrollo Científico y Tecnológico es la expresión de las aspiraciones preconizadas por los Jefes de Estado Americanos en el sentido de poner la ciencia y la tecnología al servicio de los pueblos latinoamericanos.

Demostrando gran visión, dichos dignatarios reconocieron que la ciencia y la tecnología están transformando la estructura económica y social de muchas naciones y que, en esta hora, por ser instrumento indispensable de progreso en América Latina, necesitan un impulso sin precedentes.

El Programa Regional de Desarrollo Científico y Tecnológico es un complemento de los esfuerzos nacionales de los países latinoamericanos y se orienta hacia la adopción de medidas que permitan el fomento de la investigación, la enseñanza y la difusión de la ciencia y la tecnología; la formación y perfeccionamiento de personal científico; el intercambio de informaciones, y la transferencia y adaptación a los países latinoamericanos del conocimiento y las tecnologías generadas en otras regiones.

En el cumplimiento de estas premisas fundamentales, el programa de monografías representa una contribución directa a la enseñanza de las ciencias en niveles educativos que abarcan importantísimos sectores de la población y, al mismo tiempo, propugna la difusión del saber científico.

La colección de monografías científicas consta de cuatro series, en español y portugués, sobre temas de física, química, biología y matemática. Desde sus comienzos, estas obras se destinaron a profesores y alumnos de ciencias de los primeros años de la universidad; de éstos se tiene testimonio de su buena acogida.

Este prefacio brinda al Programa Regional de Desarrollo Científico y Tecnológico de la Secretaría General de la Organización de los Estados Americanos la ocasión de agradecer al doctor Enzo R. Gentile, autor de esta monografía, y a quienes tengan el interés y buena voluntad de contribuir a su divulgación.

"Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk" (Dios creó los números naturales, el resto lo hizo el hombre).

Leopold Kronecker
21 de septiembre de 1886

INDICE

PROLOGO

La teoría de números ha ocupado siempre una posición peculiar respecto de las distintas ramas de la matemática por su reputación de ser difícil y por estar revestida de un aura de cierto misterio. Es, sin embargo, única en cuanto a campo de experimentación de la imaginación. Como ya lo señalaron Hilbert y Hardy, la teoría de números es fundamental para el entrenamiento matemático inicial. Desde el comienzo es aparente su esquema coherente, riguroso y de extrema profundidad. La teoría de números no es propia de ningún nivel educativo en especial y aun en la escuela primaria su potencialidad no ha sido realmente evaluada y aprovechada.

Desde hace años la enseñanza de la matemática en todos los niveles está en verdadera crisis: consiste en repetir libros formales con pobre ejercitación y, la mayor parte de las veces, falla en suscitar motivación. El alumno no pasa de ser un mero receptáculo de conocimientos que difícilmente puede digerir y que lo llevan rápidamente a la frustración y al fracaso. Su participación es prácticamente nula. En general, el espíritu de la matemática moderna con sus numerosas definiciones y esquemas abstractos hace que el alumno desarrolle muy pobremente su capacidad creadora y de trabajo. Por lo general, los ejemplos son escasos y muchas veces no existen. La mayor deficiencia en la enseñanza, y esto se advierte incluso en la universidad, es que se aprende teoría con muy pocos ejemplos. La teoría, los ejemplos y la resolución de problemas forman el triángulo de equilibrio de toda enseñanza eficaz. La aritmética representa una opción excelente para mejorar la enseñanza de la matemática. Su fuerza radica en la facilidad de plantear problemas de todo tipo de complejidad. El resolverlos es el ejercicio específico del aprendizaje.

La aritmética es una ciencia cotidiana, capaz de atraer a cualquier persona que posea sólo un poco de curiosidad. Observemos cómo las revistas de entretenimientos numéricos llaman la atención de mucha gente a veces con poca instrucción. ¿Por qué no explotar ese germen de curiosidad que posee la gente joven y los niños en especial? Hay que evitar llenar la cabeza de los alumnos con fórmulas y teoremas sin darles la oportunidad de pensar libremente, invitándolos a imaginar. La verdadera fuerza de la matemática es la *creación*: luego, si se quiere, se puede hablar de rigor, formalismo, didáctica o lo que sea. La aritmética no termina allí, se puede profundizar *ad infinitum*. Ramas bien establecidas generalizan la clásica teoría de números, como, por ejemplo, la teoría algebraica de números, la teoría analítica, la geometría diofantina y geometría aritmética. La misma ciencia de la computación es un aliado valiosísimo para experimentar con problemas y conjeturas. La evolución de la computación ha hecho que la artimética deje de ser una ciencia contemplativa y de especialistas para transformarse en una verdadera rama aplicada. La

necesidad de nuevos algoritmos de computación requiere vastos y profundos conocimientos aritméticos. Para dar una idea de ello se aconseja al lector consultar la colosal obra *The Art of Computer Programming*, de Donald Knuth, en tres volúmenes.

Esperamos que esta monografía proporcione al profesor material para experimentar y lo incentive a realizar una labor creadora que dé a sus alumnos la oportunidad de participar activamente.

1

ASPECTOS HISTORICOS

La teoría de números o aritmética (del griego *arithmos*, número) estudia las propiedades de los números naturales $N = \{1, 2, 3, \ldots\}$ o enteros $Z = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$. ¿Qué propiedades de los números interesa estudiar? Dos propiedades que han dado gran impulso a la aritmética son las referentes a la existencia de números primos y a la *divisibilidad* de enteros.

Los números primos encierran todo tipo de problemas. Uno de ellos, por ejemplo, se refiere a cuántos números primos hay. Euclides (s. III a. de J. C.) dio una demostración de la existencia de infinitos primos. Otra pregunta interesantes es saber cuál es el n-simo primo, o sea dar una fórmula que para cada $n \in N$, dé el n-simo primo. Por ejemplo, la fórmula $n^2 + n + 41$ da un número primo para todo n de 1 a 39. Sin embargo, para $n = 40$ resulta $40^2 + 40 + 41 = (40 + 1)^2$, no primo, y se demuestra que ningún polinomio $f(X)$ con coeficientes enteros puede satisfacer la propiedad: $f(n)$ es primo para todo $n \in N$. No se conoce ninguna fórmula satisfactoria que dé el n-simo primo.

Pierre de Fermat infirió que los números $F_n = 2^{2^n} + 1$ eran primos para todos los $n \in N$. Esta conjetura resultó errónea, pues para $n = 5$, Euler probó que F_5 es divisible por 641. Sin embargo, hasta hoy no se sabe si hay infinitos primos de la forma F_n.

Desde un punto de vista histórico puede ser razonable recordar el problema tratado por Pitágoras (580-500 a. de J. C.) sobre la construcción de triángulos rectángulos cuyos lados poseen longitudes enteras. O sea, se trata de resolver la ecuación $x^2 + y^2 = z^2$ para valores enteros de x, y y z. Por ejemplo, $3^2 + 4^2 = 5^2, \ldots$. Pitágoras obtuvo las infinitas soluciones $x = 2t$, $y = t^2 - 1$ y $z = t^2 + 1$, donde t es cualquier número entero.

Tan remotamente como 500 años a. de J. C. los chinos conocían la propiedad que si p es primo, entonces p divide a $2^p - 2$ y hasta la consideraban una regla infalible de primalidad, o sea que "p es primo si, y sólo si, p divide a $2^p - 2$". Hasta Fermat (siglo XVII) se creyó en esta propiedad. Fermat probó que si p es primo, entonces p divide a $2^p - 2$ y a partir de este resultado general se observó que el número $341 = 11 \cdot 31$ divide a $2^{341} - 2$, de manera que la afirmación de los chinos no era correcta. Es claro que para éstos hacer una verificación hubiera sido demasiado improbable dado que el número $2^{341} - 2$ tiene 103 cifras.

Se puede decir que el primer estudio sistemático de la teoría de números fue hecho por Euclides. En sus *Elementos* (Libros VII, VIII y IX dedicados a la teoría de números) aparece explícitamente el algoritmo de la división entera, la obtención del máximo común divisor a partir de ese algoritmo, la demostración de la existencia de infinitos

primos y la siguiente propiedad equivalente a la unicidad de la factorización en producto de primos: Si ninguno de dos números a y b es divisible por un primo p, tampoco lo es el producto $a \cdot b$, o su equivalente $p|a \cdot b$ implica $p|a$ o $p|b$.

Aunque puede ser objeto de controversia, se supone que, más que creador, Euclides fue un recopilador de cosas conocidas en su tiempo. No obstante, sus *Elementos* constituyen la primer obra clásica sobre la teoría de números.

El primer enunciado claro sobre la factorización única en producto de primos, es decir el llamado *Teorema Fundamental de la Aritmética*, fue hecho por Gauss en sus *Disquisitiones Arithmeticae* de 1801.

Mencionemos un resultado que aparece en uno de los *Elementos* y que dio lugar a uno de los más antiguos problemas abiertos* en la teoría de números, a saber: un número natural de la forma $2^p - 1$ es primo si, y sólo si, el número $2^{p-1} \cdot (2^p - 1)$ es *perfecto*. (Un número natural n se dice que es perfecto si la suma de todos sus divisores positivos es $2n$. Por ejemplo, $n = 6$, $n = 28$, $n = 496$, $n = 8128$.)

Posteriormente, Euler probó que si n es un número perfecto *par*, entonces tiene la forma $2^{p-1} \cdot (2^p - 1)$ con $2^p - 1$ primo. O sea, los números perfectos *pares* están completamente caracterizados. Un problema aún sin solución es saber si existen números perfectos *impares*. Otra consecuencia interesante de este resultado es que plantea la existencia de primos de la forma $2^p - 1$ (llamados primos de *Mersenne*).

Marin Mersenne (1588 - 1648), monje francés, hizo ciertas conjeturas sobre la primalidad de números de la forma: $M_n = 2^n - 1$ (números de Mersenne). En 1644 Mersenne discurrió que M_p es primo para $p = 2, 3, 5, 7, 13, 19, 31, 67, 127$ y 257 y compuesto para todos los otros primos menores que 257. Recién en 1947, gracias a las calculadoras, pudo analizarse esta conjetura. Resultó que Mersenne había cometido cinco errores: M_{67} y M_{257} *no* son primos, pero sí lo son M_{61}, M_{89} y M_{107} que habían sido excluidos de la lista.

Igualmente un problema sin solución aún es saber si existen infinitos primos de Mersenne. Nótese que si $2^p - 1$ es primo, entonces necesariamente p es primo, pues si $p = a \cdot b$, $(2^a)^b - 1$ siempre es divisible por $(2^a - 1)$. Esto es interesante pues es una manera de obtener en forma efectiva nuevos números primos. El mayor número primo de Mersenne que se conoce hasta hoy es $2^{86243} - 1$, que posee 25.962 dígitos. Los métodos modernos de computación permitirán descubrir nuevos números primos de Mersenne.

Otro matemático griego que contribuyó en forma significativa a la teoría de números es Eratostenes de Cirene (276-194 a. de J. C.). La llamada "Criba de Eratostenes" permite determinar todos los números primos menores que un número n dado. Para ello se disponen los nú-

---

* abiertos: aún sin solución.

meros naturales de 2 a n en orden creciente. Si un número entero $a >$ > 1 no es divisible por ningún primo $\leq \sqrt{a}$, entonces a es primo. Por lo tanto, conocidos los primos $p \leq \sqrt{n}$, si en aquel orden se tachan todos los múltiplos de p, mayores que p, para todos los primos $p \leq \sqrt{n}$, quedan los primos menores que n. O sea, se hace un "tamizado". Es interesante notar que este procedimiento de Eratostenes es un primer intento de estudiar la distribución de primos o, equivalentemente, la densidad de los primos en la totalidad N.

Ya en la era cristiana, como continuación de los *Elementos* de Euclides, aparece la famosa *Aritmética* de Diofanto de Alejandría (c. 250), matemático griego que vivió en Alejandría. Se la considera, además, uno de los primeros tratados de álgebra por el manipuleo "algebraico" de símbolos. Lo más relevante de la obra de Diofanto son las ecuaciones del tipo $x^2 - d \cdot y^2 = \pm 1$, y el problema de su resolución, pero en número enteros. En general, se puede afirmar que, a partir de Diofanto, el estudio de la resolución en números enteros de ecuaciones algebraicas constituye el llamado "Análisis Diofantino", importante rama actual y particularmente difícil de la teoría de números.

La aritmética, escrita originalmente en griego, fue editada por primera vez en Europa, en 1621, por Claude Gaspard de Bachet (1581-1638) en ambos textos, griego y latín. Fue precisamente esta edición la que atrajo a Fermat a la aritmética. Pierre de Fermat, llamado por algunos el padre de la teoría de números, nació en 1601, cerca de Toulouse, Francia, y pasó toda su vida en el sur de Francia, lejos de los centros europeos importantes.

Fermat trabajó como abogado y juez y tal vez buscó en la abstracción y la creación matemática refugio a sus funciones de jurista. Como éstas le demandaban gran parte del tiempo, Fermat solía escribir en los márgenes de todo libro que llegaba a sus manos. Su copia personal de la edición de Bachet de la *Aritmética* de Diofanto, contenía en sus márgenes muchos de sus famosos teoremas en teoría de números. Su hijo Samuel, cinco años después de la muerte de Fermat, acaecida en 1665, encontró esta copia y publicó una nueva edición de la *Aritmética* incorporando las notas marginales hechas por su padre. Interesa hacer notar que Fermat fue prácticamente el único en todo el siglo XVII que se ocupó de la teoría de números, y eso explica que no hubiera escrito en detalle sus resultados y que todas sus publicaciones hubieran aparecido después de su muerte. Fermat formuló una gran variedad de problemas y afirmaciones, en muchos casos sin demostración. Mencionaremos, por ejemplo, su famoso "pequeño teorema" (demostrado posteriormente por Euler): si p es primo positivo y a es un entero coprimo de p, entonces p divide a $a^{p-1}-1$, o en notación habitual: $a^{p-1} \equiv$ $\equiv 1$ módulo p.

Otro enunciado sin demostración es el siguiente: Todo número entero positivo es suma de cuatro cuadrados enteros, incluyendo el cero como cuadrado. Este resultado no fue probado sino hasta 1772 por Lagrange.

La figura señera en la matemática del siglo XVIII fue Leonhard Euler (1707-1783), quien nació en Basilea (Suiza) y pasó la mayor parte

de su vida en la Academia Imperial de San Petersburgo en Rusia y en la Academia Real de Berlín. Sin duda Euler es uno de los matemáticos más prolíficos. En 1766 quedó ciego, pero este hecho no interrumpió de manera alguna su productividad. A los fines de esta introducción histórica el hecho más saliente de la obra de Euler es haber rescatado y analizado las contribuciones de Fermat, demostrado la mayoría de sus conjeturas y establecido los cimientos científicos de la teoría de números, continuada luego con gran maestría por Gauss.

Una conjetura errónea de Fermat (en una carta a Mersenne escrita en 1640) es la que afirma que el número (de Fermat!) $2^{2^n} + 1$ es primo para todo n, agregando que "aunque convencido de su validez, no la podía probar". Posteriormente, Euler demostró que para $n = 5$, el número de Fermat correspondiente es divisible por 641. Curiosamente el mismo "pequeño teorema" de Fermat (descubierto también en el año 1640) permite mostrar la no primalidad de $2^{32} + 1$ ($n = 5$). En efecto, tal teorema da un valioso criterio de no primalidad: si p y a son números naturales coprimos tales que $a^{p-1} \not\equiv 1$ módulo p, entonces p no es primo.

Por ejemplo, si $p = 2^{32} + 1$, es claro que 3 y p son coprimos, pues $2^2 \equiv 1$ módulo 3 implica $2^{32} \equiv 1$ módulo 3, o sea $2^{32} + 1 \equiv 2$ módulo 3. Si se aplica este criterio, se verifica que $3^{2^{32}} \not\equiv 1$ módulo $2^{32} + 1$, de manera que este último no es primo.

Cabe mencionar también que Fermat efectuaba muchas demostraciones por el método denominado "del descenso infinito" *(descente infinie)** que hoy no es otra cosa que el principio de buena ordenación (todo conjunto no vacío de números naturales posee un número mínimo).

Todo este fárrago de resultados e información fue más tarde analizado por Euler, quien fascinado por los enunciados de Fermat, se consagró a la tarea de demostrarlos no sin antes reconstruir todos los hechos básicos que hoy encontramos tan claramente expuestos en los textos elementales sobre la teoría de números.

En el ejemplar de Bachet del libro de Diofanto, en una parte donde se plantea el problema de hallar cuadrados que son sumas de dos cuadrados, Fermat escribió: "Por otra parte, es imposible para un cubo ser suma de dos cubos, para una cuarta potencia ser suma de dos cuartas potencias o, en general, para un número que es potencia mayor que 2 ser suma de dos números que son de esta misma potencia. He descubierto una demostración maravillosa de esta afirmación imposible de escribir en este estrecho margen". Simbólicamente, esa proposición, hoy llamada el *Ultimo Teorema de Fermat* o la *Conjetura de Fermat* (C. F.) establece que si n es un número natural mayor que 2 no existen números naturales x, y y z que satisfagan la ecuación $x^n + y^n = z^n$. Este es uno de los problemas abiertos más famosos en matemática. Es claro

* El método del descenso infinito puede enunciarse aproximadamente así: Si, suponiendo que un problema admite una solución entera $n > 0$, deducimos que posee una solución entera $n' > 0$, $n' < n$, entonces el problema no admite soluciones enteras positivas.

que para la resolución de la conjetura de Fermat basta limitarse a exponentes $n = 4$ o n = primo impar. En efecto, si la conjetura de Fermat ha sido probada para un cierto n, queda automáticamente establecida para todo múltiplo, dado que si $m = n \cdot n'$: $x^m + y^m = z^m$ implica $(x^{n'})^n + (y^{n'})^n = (z^{n'})^n$. El propio Fermat obtuvo una demostración para $n = 4$ a partir de su famoso método del descenso y para $n = 3$ fue Euler quien lo demostró. Uno de los hechos relevantes de la demostración de Euler consiste en usar números complejos de la forma $a + b \cdot \sqrt{-3}$, donde a y b son enteros. La totalidad de números de esta forma constituye un anillo $Z[\sqrt{-3}]$. Euler imita la aritmética de Z en $Z[\sqrt{-3}]$, pero con la ingenuidad de suponer que en $Z[\sqrt{-3}]$ es válido un teorema fundamental de la aritmética, es decir, representación única en producto de primos. Pero esto no es así y el razonamiento de Euler no es correcto, aunque se puede subsanar para lograr la demostración. Curiosamente, errores famosos en el mismo contexto de la factorización se produjeron más tarde en los múltiples intentos que se hicieron para resolver la conjetura de Fermat, errores que, sin embargo, constituyeron los gérmenes del desarrollo de la teoría algebraica de números.

En 1820, Gustav Lejeune Dirichlet (matemático alemán, 1805-1859) y Adrien-Marie Legendre (matemático francés, 1752-1833) probaron independientemente la conjetura de Fermat para el siguiente número primo, es decir $n = 5$. El método de demostración fue esencialmente el utilizado por Euler. Quince años más tarde el matemático francés Gabriel Lamé (1775-1870) dio una compleja y extensa demostración del caso $n = 7$, pero quedaron dudas sobre la posibilidad de extender su método a $n = 11$. La necesidad de introducir nuevas ideas era aparente. El mismo Lamé, tratando el problema general, retoma una idea de Lagrange (Joseph Louis, nacido en Turín, Francia, 1736-1813), quien señaló la posibilidad de introducir raíces n-simas de la unidad en el estudio del Problema de Fermat. Sea, en efecto, $w = w_n$ una raíz n-sima primitiva de la unidad. Puesto que n es impar, se puede escribir $z^n = x^n + y^n = x^n - (-y)^n = (x + y) \cdot (x + w \cdot y) \ldots (x + w^{n-1} \cdot y)$.

Para precisar mejor el contexto en que se está discurriendo digamos que la adjunción de w al cuerpo racional Q produce una extensión algebraica de grado $n-1$ sobre Q (dado que n es primo). Los elementos de $Q(w)$ son los números complejos de la forma $a_0 + a_1 \cdot w + \ldots + a_{n-1} \cdot w^{n-1}$, con a_i racional. Dentro de este cuerpo se encuentran los llamados enteros algebraicos de $Q(w)$, que resultan ser la totalidad $Z[w]$ de expresiones del tipo anterior, donde los a_i son todos enteros racionales. Cabe entonces pensar que la factorización anterior tiene lugar en el anillo $Z[w]$. Adelantemos el resultado fundamental de Kummer que, si $Z[w]$ es un dominio de factorización única, la conjetura de Fermat para el n primo correspondiente es verdadera. Recién en 1972 se demostró que sólo para los primos menores que 23, $Z[w]$ es de factorización única. Hagamos una observación respecto al caso $n = 3$. El anillo de enteros algebraicos de $Q(w)$, $w = \dfrac{-1 + \sqrt{-3}}{2}$, es la totalidad de complejos de la forma $a + b \cdot w$, a y b enteros que, a su vez, coincide con la totalidad de complejos de la forma $\dfrac{a + b \cdot \sqrt{-3}}{2}$, donde a y b son enteros que po-

seen la misma paridad. Este anillo (pero *no* $Z[\sqrt{-3}]$) es de factorización única. Respecto a este anillo, Gauss da otra demostración de la Conjetura de Fermat para $n = 3$ y completa así la demostración de Euler.

Una de las consecuencias más importantes del "Ultimo Teorema de Fermat" es haber planteado una cuestión vital para la teoría de números, más importante quizá que el mismo Teorema de Fermat, a saber: ¿para qué primos p es $Z[w_p]$ un dominio de factorización única? Más aún, puede decirse que el mismo problema subsiste para dominios numéricos en general. La factorización única en el anillo de enteros Z es hasta cierto punto excepcional y es una propiedad que debe destacarse. Es probable que Gauss haya sido el primer matemático con ideas claras acerca de la unicidad de la factorización. En efecto, Gauss probó que el anillo $Z[i] = \{ a + b \cdot i \mid a, b \in Z,\ i^2 = -1\}$ es un dominio de factorización única. Es el llamado anillo de *enteros de Gauss*.

La mayor contribución de todos los tiempos al problema de Fermat se debe al matemático alemán Ernst Eduard Kummer (1810-1893). Su estudio profundo y original de los *números ciclotómicos* (o sea de la aritmética de $Z[w]$) le permitió dar una condición suficiente sobre el primo n para que la conjetura de Fermat sea válida. Para dichos primos, llamados *regulares*, se sigue la validez del teorema de Fermat. Digamos que, además de los casos $n = 3$, 5 y 7, el método de Kummer permitió probar la conjetura en el rango 3-100 para todos los primos excepto tres de ellos (¡primos irregulares!), a saber 37, 59 y 67.

Volviendo a la idea de trabajar con enteros ciclotómicos, imitando la teoría que Euler había ideado con los números del tipo $a + b \cdot \sqrt{-3}$, Lamé propuso aplicar la "unicidad de la factorización en productos de primos en $Z[w]$" a la resolución del problema de Fermat. Digamos que la propiedad esencial requerida de un dominio de factorización única es la que establece que si $a \cdot b = c^n$ y a y b son coprimos, entonces $a = u \cdot a_1^n$ y $b = u' \cdot b_1^n$, donde u y u' son elementos inversibles (o sea unidades del dominio en cuestión). Anteriormente señalamos que no todo $Z[w]$ es de factorización única y Lamé produjo un gran fiasco al anunciar en la Academia de Ciencias de París la solución, con estas ideas, de la conjetura de Fermat, y al publicarlas posteriormente en los *Comptes Rendus* de la Academia de Ciencias de París (Lamé, G. Démostration générale du théorème de Fermat sur l'impossibilité en nombres entiers de l'équation $X^n + Y^n = Z^n$, *Compt. Rend., Acad. Sci. Paris*, **24**, 310-314, 1847).

La conjetura de Fermat no ha sido resuelta aún, pero ha generado importantes teorías y dado lugar a otros problemas que son, en definitiva, el alma de la matemática.

El gran matemático alemán Carl Friedrich Gauss (1777-1855) en su obra monumental *Disquisitiones Arithmeticae* aparecida en 1801, cuando Gauss tenía 24 años, fijó las bases fundamentales de la moderna teoría de números. Uno observa que la aritmética antes de Gauss, más que una ciencia parece una suerte de hechos aislados y anecdóticos, y que Gauss la eleva a su verdadera dimensión científica.

Disquisitiones Arithmeticae reúne la obra en aritmética de los predecesores de Gauss, pero la enriquece en tal magnitud que sin lugar a dudas marca el inicio de la moderna teoría de números. Comienza con la exposición de la noción de relación de congruencia entera, la teoría de residuos cuadráticos, formas cuadráticas y cuerpos ciclotómicos.

Fue Gauss quien definió la noción de congruencia de números e introdujo la notación utilizada en la actualidad. Si m es un número entero positivo, se dice que dos números a y b son *congruentes módulo m* si su diferencia $a - b$ es divisible por m. La notación de Gauss destaca la estrecha analogía con la igualdad

$$a \equiv b (\text{mód. } m)$$

La definición de congruencia clasifica a los números enteros según los posibles restos en la división por m, o sea $a \equiv b(\text{mód. } m)$ si, y sólo si, a y b tienen el mismo resto en la división "entera" por m. Si $m = p_1^{r_1} \dots p_s^{r_s}$ es la factorización de m en producto de primos, $p_i \neq p_j$ si $i \neq j$, entonces la congruencia anterior se reduce al sistema de congruencias $a \equiv b$ (módulo $p_i^{r_i}$).

Por ser tan común en la matemática actual podría pensarse que éste constituye un primer resultado sobre "localización" (reducción a las componentes primas). Digamos que en las congruencias se tiene una forma efectiva de cálculo que la computación actual sabe aprovechar. Por ejemplo, sea $m = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. Es fácil ver que $a \equiv b$ módulo 210 si, y sólo si, $a \equiv b$ módulos: 2, 3, 5, 7. En particular, si a y b son números naturales menores que 210, se tiene que $a = b$ si, y sólo si, $a \equiv b$ módulos 2, 3, 5 y 7, respectivamente. Por lo tanto, toda la aritmética entre 0 y 210 puede hacerse si se trabaja con enteros módulos 2, 3, 5 y 7 (Teorema Chino del Resto).

Gauss consideró asimismo las ecuaciones algebraicas de congruencias $f(x) = a_n x^n + \dots + a_1 x + a_0 \equiv 0$ módulo m, donde las a_i son enteros, y el problema consiste en resolverlas mediante soluciones enteras. Aquí el problema puede reducirse, como se señaló antes, a la situación $m = p^s$, p primo. Por ejemplo, la ecuación $f(X) = X^n - a \equiv 0$ módulo m, con a no divisible por m. Cuando dicha ecuación tiene solución entera se dice que a es un residuo de n-simo grado, y si $n = 2$, se dice que es un *residuo cuadrático*. Con anterioridad Legendre había inventado la notación $(\frac{a}{p})$ para p primo impar y a cualquier entero coprimo con p, para designar a la función $(\frac{a}{p}) = 1$, si a es residuo cuadrático módulo p, y $(\frac{a}{p}) = -1$, si a no es residuo cuadrático módulo p. Legendre (1785) ideó, probablemente basado en observaciones empíricas de Euler (1783), la siguiente fórmula:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

si p y q son primos positivos impares y la llamó *ley de reciprocidad para residuos cuadráticos*. Dicha ley, completada con las siguientes *leyes complementarias*

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$$

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$$

(p primo impar)

permite calcular $(\frac{a}{p})$ para cualquier primo p y cualquier entero a, coprimo con p.

Legendre demostró esta ley en una memoria titulada *Recherches d'Analyse Indéterminée* (1785), pero, como Gauss afirma en sus *Disquisitiones*, dicha demostración es incompleta, pues utiliza sin demostración el siguiente (y luego famoso) resultado denominado "Teorema de los primos en una progresión aritmética" (T. P. P. A.).

(T. P. P. A.): dados a y b enteros coprimos, la sucesión $a+b$, $a+2b$, $a+3b, \ldots a+n \cdot b, \ldots$ contiene infinitos primos. Es decir, si a y b son enteros coprimos hay infinitos primos de la forma $a+n \cdot b$. Cabe añadir que Legendre hizo una exposición sistemática y más completa de sus *Recherches* en *Essai sur la Thèorie des Nombres*, obra publicada en 1798 y subsecuentemente ampliada en su famosa *Thèorie des Nombres*. Las investigaciones de Legendre inspiraron en buena medida a Gauss en sus *Disquisitiones*. Ambas publicaciones fueron durante mucho tiempo las obras de consulta de rigor en la teoría de números.

Gauss asignó gran importancia a la ley de reciprocidad a la que llamó *Theorema fundamentale theoriae residuorum quadraticorum*, y en el curso de su vida dió siete demostraciones completas de ella sin utilizar el teorema de los primos en una progresión aritmética y la llamó también *Ley de Reciprocidad Cuadrática* (L. R. C.). Se dice que hasta el presente se han dado no menos de 150 demostraciones distintas.

La formulación de Gauss de la L. R. C. es la siguiente: "Sean p y q primos positivos impares. Si p es de la forma $4m+1$, entonces la ecuación $X^2 \equiv q$ (mód. p) admite solución si, y sólo si, la ecuación $X^2 \equiv p$ (mód. q) admite solución. Si p es de la forma $4m+3$, entonces la ecuación $X^2 \equiv q$ (mód. p) admite solución si, y sólo si, la ecuación $X^2 \equiv -p$ (mód. q) admite solución".

La ley de reciprocidad cuadrática determina completamente para cada entero a la factorización del polinomio $X^2 - a$ sobre los cuerpos primos Z_p de enteros módulo p. Por ejemplo, si $a = 17$, el polinomio $X^2 - 17$ es factorizable en Z_p, p primo impar $\neq 17$, si, y sólo sí, $(\frac{17}{p}) = 1$. *A priori* habría que analizar los símbolos $(\frac{17}{p})$ para infinitos primos p. Sin embargo, la ley de reciprocidad cuadrática dice que $(\frac{17}{p}) \cdot (\frac{p}{17}) = 1$, es decir $(\frac{17}{p}) = (\frac{p}{17})$, por lo tanto el carácter de ser 17 residuo cuadrático módulo p está determinado por el carácter de ser p

residuo cuadrático módulo 17. Puesto que los cuadrados no nulos módulo 17 son 1, 2, 4, 8, 9, 13, 15 y 16, se tiene que el polinomio $X^2 - 17$ es factorizable en Z_p, p primo impar, si, y sólo si, $p \equiv 1, 2, 4, 8, 9, 13, 15, 16$, módulo 17.

La ley de reciprocidad cuadrática es el resultado clásico más importante a partir del cual se desarrolla sistemáticamente la teoría de números. El esfuerzo reside en obtener leyes de reciprocidad de grado superior. Por ejemplo, dado un entero k y un número primo p ¿qué puede decirse de la resolubilidad de la congruencia $x^4 \equiv k$(mód. p)? La búsqueda de leyes de reciprocidad como también el intentar resolver el Ultimo Teorema de Fermat han dado lugar a un extraordinario auge de dos ramas de la teoría de números: la teoría algebraica de números y la teoría analítica de números. Cabe decir que el descubrimiento de Kurt Hensel de los números p-ádicos y de los métodos p-ádicos ha enriquecido el enfoque y desarrollo de la aritmética.

Se dijo antes que Legendre, en su demostración de la ley de reciprocidad cuadrática, supuso la propiedad de existencia de infinitos primos en las progresiones aritméticas $a + n \cdot b$, si a y b son enteros positivos coprimos. Este resultado, no demostrado, motivó a Dirichlet a idear nuevos métodos en la teoría de números que dieron lugar al nacimiento de lo que hoy se llama Teoría Analítica de Números. Dirichlet fue un apasionado lector de *Disquisitiones Arithmeticae* y trató de simplificar muchos de los resultados allí contenidos. Los trabajos de Dirichlet en teoría analítica están influenciados por algunos resultados de Euler relativos a series. Gottfried Wilhelm Leibniz (1646-1716) concibió la serie

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$$

Euler, fascinado por este tipo de resultados, llegó a un resultado importante, a saber la serie

$$\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots$$

Esta y otras series análogas lo condujeron a la "función zeta"

$$Z(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s \in R, \quad s > 1$$

y a su famosa fórmula

$$Z(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \Pi_p (1 - \frac{1}{p^s})^{-1}, \quad s \in R, \quad s > 1$$

El producto es infinito y p recorre todos los primos positivos.

Cuando s tiende a 1 por la derecha, se obtiene una nueva demostración de la infinitud del número de primos racionales, muy distinta de las ya conocidas.

En forma análoga, Dirichlet definió L-funciones $L(s, \chi)$ como sigue: Sea Z_m^* el grupo multiplicativo de enteros inversibles módulo m, o sea lo que suele llamarse el grupo de unidades del anillo Z_m. Sea $\chi : Z_m^* \to C^*$ un morfismo del grupo Z_m^* en el grupo de números complejos no nulos. Un tal morfismo se denomina un *carácter* de Z_m^*. En particular, si $\chi(t) = 1$, se obtiene de modo idéntico el carácter trivial χ_0. Un carácter χ de Z_m^* se extiende a una función sobre el anillo Z como sigue

$$\chi(n) = \begin{cases} \chi(\bar{n}), & \text{si } (n,m) = 1 \\ 0, & \text{en otro caso} \end{cases}$$

($\bar{n}$ denota la clase de n módulo m).

Se define, entonces, $L(s, \chi)$ por la serie

$$L(s, \chi) = \sum_{n \in N} \frac{\chi(n)}{n^s}, \quad s \in R, \quad s > 1$$

Estas series son absolutamente convergentes para todo $s > 1$ y además son funciones continuas de s, si $s > 1$. Dado el carácter multiplicativo de χ, se deduce una fórmula análoga a la de Euler

$$L(s, \chi) = \pi_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \quad s > 1$$

Con estas funciones se establece el teorema de los primos en una progresión aritmética. Los detalles pueden consultarse, por ejemplo, en K. Chandrasekharan, *Introduction to Analytic Number Theory*, Springer-Verlag, 1968.

Es interesante observar cómo el análisis se inserta naturalmente en la aritmética permitiendo cierto tratamiento global. Los hechos relatados más arriba dieron origen a métodos analíticos en la teoría de números, pero no sólo de números enteros, sino de otros dominios numéricos y de funciones algebraicas. La influencia de G. F. B. Riemann (1826-1866) afianzó y dió nuevo vigor a aquellas ideas. En una memoria famosa "Über die Anzahl der Primzahlen unter einer gegeben Grösse", de 1859, Riemann extiende la función zeta de Euler a todo el plano complejo y obtiene una función analítica con un único polo simple en el complejo 1, intuyendo la verdadera relación de esta función con la distribución de primos racionales.

Denotemos por $\pi(x)$, x real, el número de primos positivos menores que x. Uno de los primeros problemas en la teoría de números ha sido indudablemente lograr alguna información sobre esta función. Por medios empíricos, utilizando sobre todo tablas, se sospechó desde muy temprana fecha que la función $\pi(x)$ se comporta "asintóticamente" como la función $\frac{x}{\ln(x)}$ en el sentido que

$$\text{lím}_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1 \qquad [P]$$

Curiosamente, el comportamiento de la función zeta de Riemann en la recta $1 + t \cdot i$ tiene que ver con la distribución de los números primos. En efecto, la afirmación [P] es enteramente equivalente a que $Z(1 + t \cdot i) \neq 0$ para todo $t \in R$. La afirmación [P] se denomina el *Teorema de los Números Primos* y fue demostrada en 1896, independientemente, por los matemáticos Jacques Hadamard (1865-1963) y Charles de la Vallée-Poussin (1866-1962) francés y belga, respectivamente. Una formulación equivalente a [P] es que el n-simo primo p_n es asintóticamente igual a $n \cdot \ln(n)$. Se sigue del teorema de los números primos que, por ejemplo, sólo el 1% aproximadamente de los números positivos menores que e^{100} son primos.

Un último punto de esta reseña histórica se refiere a la resolución de ecuaciones algebraicas. Dado un polinomio $f(X, Y)$ en dos variables X e Y independientes y con coeficientes *enteros*, se trata de hallar *todas* las soluciones racionales de la ecuación $f(X, Y) = 0$, es decir todos los pares (x, y) de números racionales tales que $f(x, y) = 0$. Geométricamente se trata de hallar, dada una curva algebraica en el plano R^2, todos los puntos de la misma que poseen ambas coordenadas racionales. Por ejemplo, en esta monografía se da la solución completa de la ecuación $X^2 + Y^2 = 1$, que equivale a resolver en números enteros la ecuación $X^2 + Y^2 = Z^2$.

Citemos la ecuación fermatiana

$$X^n + Z^n = 1$$

La famosa conjetura de Fermat establece que si $n > 2$, no existe ningún punto racional (x, y), $x \neq 0$ e $y \neq 0$, en esta curva.

En 1908, el matemático noruego Axel Thue (1863-1922) concibió la siguiente ecuación homogénea:

$$a_0X^n + a_1X^{n-1}Y + \dots + a_nY^n = c \qquad [1]$$

donde: $n \geq 3$ y los a_i $(i = 0, \dots, n)$ y c son *enteros*. El miembro izquierdo de [1] es un polinomio homogéneo de grado n en las variables X e Y con coeficientes enteros. Si este polinomio es *irreductible*, en el sentido de no ser factorizable en producto de dos polinomios con coeficientes enteros de grado inferior a n, el teorema de Thue establece que la ecuación [1] admite *sólo un número finito de soluciones enteras*. Se sigue, en particular, que para cada entero c y $n > 2$, la ecuación $X^n + Y^n = c^n$ admite sólo un número finito de soluciones enteras.

En 1922, el matemático inglés L. J. Mordell enunció una famosa conjetura sobre el número de soluciones racionales de curvas algebraicas: Si $f(X, Y) = \sum_{i,j} a_{ij}X^iY^j$ es un polinomio con coeficientes racionales, se define *grado* de $f(X, Y)$ como el máximo valor $i + j$ de los términos $a_{ij}X^iY^j$ con $a_{ij} \neq 0$. La conjetura de Mordell establece "aproximadamente" que si el grado de una curva algebraica $f(X, Y) = 0$ con coeficientes racionales es mayor que 3, entonces la misma posee a lo sumo un número finito de puntos racionales. Se dice "aproximadamen-

te" porque la curva debe satisfacer condiciones de regularidad. (La afirmación precisa establece que una curva proyectiva no singular, definida sobre el cuerpo racional y de género mayor que 1, posee a lo sumo un número finito de puntos racionales).

En 1983, el matemático alemán Gerd Faltings probó la validez de la Conjetura de Mordell. Se sigue, en consecuencia, que para cada $n \geq 3$, la ecuación fermatiana $X^n + Y^n = Z^n$ posee sólo un número finito de soluciones enteras, lo cual desde Kummer representa sin duda el mayor avance en la resolución del problema de Fermat. La interrelación bosquejada entre aritmética y geometría forma parte de una nueva rama de la geometría, denominada *Geometría Diofantina.*

BREVE TABLA CRONOLOGICA DE AUTORES IMPORTANTES

Euclides de Alejandría (300 a. de J. C.)
Diofanto de Alejandría (250 a. de J. C.)
Pierre de Fermat (1601-1665)
Leonhard Euler (1707-1783)
Joseph-Louis de Lagrange (1736-1813)
Adrien-Marie Legendre (1752-1833)
Karl Friedrich Gauss (1777-1855)
Carl Gustav Jacob Jacobi (1804-1851)
Peter Gustav Lejeune Dirichlet (1805-1859)
Ernst Eduard Kummer (1810-1893)
Gotthold Eisenstein (1823-1852)
Leopold Kronecker (1823-1891)
Bernhard Riemann (1826-1866)
Richard Dedekind (1831-1916)
Adolf Hurwitz (1859-1919)
Kurt Hensel (1861-1941)
David Hilbert (1862-1943)
Hermann Minkowski (1864-1909)
Emil Artin (1898-1962)
Helmut Hasse (1898-1979).

2

DIVISIBILIDAD EN EL CONJUNTO Z DE ENTEROS RACIONALES

Sean a y b enteros. Sea $a \neq 0$.

2. 1. **Definición.** Se dice que a divide a b o que a es factor de b, o que a es divisor de b en Z, si existe $c \in Z$ tal que $b = a \cdot c$. En este caso, también se dice que b es múltiplo de a o que b es divisible por a. Esto se denota con el símbolo $a \mid b$ y con $a \nmid b$ la negación de $a \mid b$.

2. 2. **Ejemplos**

1. Si $a \neq 0$, $a \mid a$ y $a \mid a \cdot c$ cualquiera que sea $c \in Z$, en particular $a \mid a^2$ y $a \mid a^3, \ldots, a \mid a^n$, si $n \in N$,

2. cualquiera que sea $x \in Z$, $1 \mid x$ y $-1 \mid x$,

3. si $a \neq 0$, $a \mid -a$ y $-a \mid a$, también $a \mid o$.

4. si $a \neq 0$, $a \mid |a|$ y $|a| \mid a$.

Se sigue que todo $a \neq 0$ posee por lo menos los siguientes divisores:

$$1, \ -1, \ a, \ -a$$

A tales divisores de a los llamaremos divisores *impropios* de a. Si existen divisores de a que no son impropios, los llamaremos *propios*. Por ejemplo, 2, -2, 3, -3 son divisores propios de 6, en tanto que 2, 3, -2, -3, 4, -4, 6, -6 son divisores propios de 12.

5. $a \in N$, $a \mid 1 \Rightarrow a = 1$. En efecto, $1 = a \cdot b$, $b \in N$. Si $b = 1$, entonces $a = 1$. Si $b \neq 1$, por ser número natural $b > 1$. Por lo tanto $a \cdot b > a$, es decir $1 > a$, lo que es absurdo.

2. 3. **Ejercicios**

1. $a, b, c \in Z$. Probar que si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

2. $a, b \in Z$. Probar que si $a \mid b$ y $b \mid a$, entonces $a = b$ o $a = -b$.

3. Si $a \in Z$, $a \mid 1$, entonces $a = 1$ o $a = -1$.

4. Si $a \mid b$ y $a \mid c$, entonces $a \mid b + c$ y $a \mid b - c$.

5. Si $a \mid b + c$ y $a \mid b$, entonces $a \mid c$.

Nota: La designación Z para los números enteros proviene del vocablo alemán *Zahl* (= número).

6. ¿Es cierto que si $a \mid b \cdot c$, entonces $a \mid b$ o $a \mid c$?
¿Es cierto que si $a \mid b + c$, entonces $a \mid b$ o $a \mid c$?
¿Es cierto que si $a \mid b$ y $c \mid b$, entonces $a \cdot c \mid b$?

7. Probar que $a \mid b$ si, y sólo si, $a \mid |b|$.

8. Probar que $a \mid b$ si, y sólo si, $|a| \mid b$.

9. Probar que $a \mid b$ si, y sólo si, $|a| \mid |b|$.

10. Probar que para todo $n \in N$, $4^n - 1$ es divisible por 3. (**Solución.** Razonando "inductivamente", si $n = 1$, se trata de ver si $4^1 - 1$ es divisible por 3. Esto es cierto. Supongamos cierto que $4^n - 1$ es divisible por 3. Se tratará de probar que $4^{n+1} - 1$ es divisible por 3. Para ello se escribe:

$$4^{n+1} - 1 = 4 \cdot 4^n - 4 + 4 - 1 = 4 \cdot (4^n - 1) + 3$$

$4^n - 1$ es divisible por 3, al igual que $4 \cdot (4^n - 1)$; además, 3 es divisible por 3, por lo tanto la suma $4 \cdot (4^n - 1) + 3 = 4^{n+1} - 1$ es divisible por 3. Esto prueba la validez del paso inductivo y la afirmación es, en virtud del Principio de Inducción, válida cualquiera que sea n.)

11. Probar que para todo $n \in N$, $3^{2n+1} + 2^{n+2}$ es múltiplo de 7. (**Solución.** Para $n = 1$, se tiene $3^{2.1+1} + 2^{1+2} = 27 + 8 = 35 = 7 \cdot 5$ y la afirmación es válida. Sea, entonces, válida para n y se probará para $n + 1$.

Se escribe:

$$3^{2.(n+1)+1} + 2^{(n+1)+2} = 3^{2n+1+2} + 2^{n+2+1} =$$

$$= 3^{2n+1} \cdot 3^2 + 2^{n+2} \cdot 2 =$$

$$= 3^2 \cdot (3^{2n+1} + 2^{n+2}) - (3^2 - 2) \cdot 2^{n+2} =$$

$$= 3^2 \cdot (3^{2n+1} + 2^{n+2}) - 7 \cdot 2^{n+2}$$

y de aquí resulta inmediatamente la validez de la afirmación para $n + 1$ y, por lo tanto, la misma es cierta cualquiera que sea $n \in N$.)

12. Probar que cualquiera que sea $n \in N$:

i) $3^{2n+2} + 2^{6n+1}$ es un múltiplo de 11,
ii) $3^{4n+2} + 2 \cdot 4^{3n+1}$ es múltiplo de 17,
iii) $2^{2n-1} \cdot 3^{n+2} + 1$ es divisible por 11,
iv) $3^{2n+2} - 8n - 9$ es divisible por 64,
v) $5^{5n+1} + 4^{5n+2} + 3^{5n}$ es divisible por 11,
vi) $n^2 - 2$ *no* es divisible por 3.

13. Probar que cualquiera que sea $n \in N$, el número $7^{2n+1} - 48n - 7$ es divisible por 288.

14. Probar que cualquiera que sea $n \in N$, el número $3 \cdot 5^{2n+1} + 2^{3n+1}$ es divisible por 17.

15. i) Sean $m, a_1, \ldots, a_n$ enteros positivos tales que $m = a_1 + \ldots + a_n$. Probar que

$$\frac{m!}{a_1!\ a_2!\ \ldots\ a_n!} \in N$$

(**Sugerencia.** Expresar la fracción como producto de números combinatorios.)

ii) Probar que $\forall\, m \in N$, el producto de m enteros consecutivos, es divisible por $m!$

iii) Probar que si $m,\ n \in N$, entonces $(mn)!$ es divisible por $(m!)^n \cdot n!$ (**Solución.** Razonemos inductivamente en n. Para $n = 1$ se cumple. Entonces:

$$\frac{(m(n+1))!}{(m!)^{n+1} \cdot (n+1)!} = \frac{(mn)!\ (mn+1) \ldots (mn+m)}{(m!)^n \cdot n!\ \cdot m!\ (n+1)}$$

$$\frac{(mn!)}{(m!)^n \cdot n!}\ \frac{(m+n+1 \ldots (mn+m-1)}{(m-1)!}$$

Por hipótesis inductiva, la primera fracción es un entero y la segunda es un entero por ii.)

iv) Probar que $(n!)^2$ divide a $(2n)!$ y $\frac{(2n)!}{(n!)^2}$ es par.

v) Probar que si $n, m \in N$, entonces $(2m)! \cdot (2n)!$ es divisible por $m! \cdot n! \cdot (m+n)!$

vi) Sean $a, n, k \in N$. Probar que $a^{2^{n+k}} - 1$ es divisible por $a^{2^n} + 1$.

vii) Calcular a y b, sabiendo que $(a+b)^2 = 2304$ y que $a^2 + b^2 = 1250$.

viii) Para qué valores de n:

$n - 2$ divide a $2n$,
$n - 2$ divide a $n + 2$,
$n - 2$ divide a $n^2 - 3$.

ix) Se quiere embaldosar el plano con polígonos regulares iguales colocados de manera tal que los polígonos adyacentes tengan un solo lado en común. ¿Cuál es el número posible de lados de los polígonos? (**Respuesta:** 3, 4, 6.)

17. Probar que no existen enteros positivos a, b, c, n, con $c \leq n$, tales que $a^n + b^n = c^n$. (**Sugerencia.** Supongamos $a \leq b < c$. Entonces $b + 1 \leq c$ y, por lo tanto, $(b+1)^n \leq c^n$, o sea $b^n + n \cdot b^{n-1} + \ldots \leq c^n$. Por lo tanto, $a^n \leq b^n < n \cdot b^{n-1} \leq c^n - b^n = a^n$.)

18. Probar que:

i) 1 sumado al producto de cuatro enteros consecutivos da un cuadrado;

ii) 1 sumado al producto de dos enteros impares consecutivos o de dos enteros pares consecutivos da un cuadrado.

iii) El producto de cuatro enteros positivos consecutivos no puede ser un cuadrado.

19. i) Sea $f : N \to N$ la aplicación definida por: $f(n) = \frac{n}{2}$ si n es par, $f(n) = 3n + 1$ si n es de la forma $n = 4k + 1$ y $f(n) = 3n - 1$ si n es de la forma $n = 4k + 3$. Probar que para todo $n \in N$ existe $i \in N$ tal que $f^i(n) = 1$. Notación: f^i denota la composición de f con sí misma i veces. Por ejemplo: $7 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$.

ii) Sea $f : N \to N$ la aplicación definida por $f(n) = \frac{n}{3}$ si n es divisible por 3, $f(n) = 2n + 1$ si n es de la forma $n = 3k + 1$ y $f(n) = 2n - 1$ si n es de la forma $n = 3k + 2$. Probar que para todo $n \in N$ existe $i \in N$ tal que $f^i(n) = 1$.

iii) Inventar otros ejemplos.

iv) Un caso difícil: *Algoritmo de Siracusa*. Sea $f : N \to N$ definida por $f(n) = \frac{n}{2}$ si n es par y $f(n) = 3n + 1$ si n es impar. Es un problema aún no resuelto saber si para todo $n \in N$ existe $i \in N$ tal que $f^i(n) = 1$. Comprobar para $n = 31$ y $n = 41$. (Ha sido verificado afirmativamente para todos los $n \leq 2^{50}$.)

20. Sea a un entero impar. Probar que:

i) $a^2 - 1$ es divisible por 8;

ii) $a^4 - 1$ es divisible por 16 y

iii) para todo $n \in N$, $a^{2^n} - 1$ es divisible por 2^{n+2}.

21. Probar la siguiente afirmación: el producto de dos números que son suma de dos cuadrados es un número que es suma de dos cuadrados. (Sugerencia. Usar números complejos $a + b \cdot i$ y la propiedad multiplicativa de la norma $N(a + b \cdot i) = a^2 + b^2$).

22. Probar que para todo $n \in N$, el número $(3 + \sqrt{5})^n + (3 - \sqrt{5})^n$ es entero divisible por 2^n.

2.4. Números Primos - Definición. Se denomina *número primo* a todo número entero que posee exactamente cuatro divisores. O sea, si a es el número, sus divisores son: $1, -1, a$ y $-a$, todos distintos entre sí.

Esta definición puede parecer artificial, pero no lo es y, en todo caso, equivale a la dada en 1927 por Edmund Landau en su famosa "Teoría Elemental de Números".

Un número que no es ni 1, ni 0, ni -1, se dirá *compuesto* si no es primo.

Dos números a y b se dirán *coprimos* o *primos entre sí* si satisfacen:

$$d \mid a \text{ y } d \mid b \rightarrow d = 1 \text{ o } d = -1$$

Por ejemplo, si p y q son dos números primos positivos distintos, p y q son coprimos. En efecto, los divisores de p son 1, -1, p, $-p$, en tanto que los de q son 1, -1, q, $-q$. Los únicos factores comunes a p y a q son 1 y -1. En cambio, 6 y 15 no son coprimos, pues 3 es divisor común y $3 \neq 1$ y $3 \neq -1$.

2.5. Ejemplos

1. 1 no es primo, pues posee sólo dos divisores: 1 y -1;
-1 no es primo, pues posee sólo dos divisores: 1 y -1;
0 no es primo, pues posee más de cuatro divisores (cualquier entero no nulo divide a 0).

2. 2, 3 y 5 son números primos, pues tienen cuatro divisores.

3. 3 es primo. En efecto, $a \cdot b = 3$ y $a > 1$ implican $b > 0$ y, por lo tanto, $3 = a \cdot b > 1 \cdot b = b$, con lo que $b = 1$ o $b = 2$. Si $b = 2$, $a > 1$ implica $a \geq 2$ y, por lo tanto, $3 = a \cdot b \geq 2 \cdot 2 = 4$, lo que es absurdo. Se sigue que $b = 1$, con lo que $a = 3$. Si $a < 0$, se escribe $3 = (-a) \cdot (-b)$ y se vuelve al caso anterior, por lo tanto $-a = 1$ o $-a = 3$, es decir $a = -1$ o $a = -3$. Los divisores son los impropios. 3 es primo.

2.6. **Proposición.** Sean a, b y c números naturales. Entonces, $a = b \cdot c$ implica $b \leq a$ y $c \leq a$.

Demostración. Tratándose de números naturales:

$1 \leq b$, por lo tanto $c \cdot 1 \leq c \cdot b$, o sea $c \leq a$,
$1 \leq c$, por lo tanto $b \cdot 1 \leq b \cdot c$, o sea $b \leq a$.

2.7. **Proposición.** Sea $a \in Z$. Si $a \neq 1, -1, 0$ y a no es un número primo, existe $t \in N$ tal que $1 < t < |a|$ y $t \mid a$.

Demostración. Sea $a = r \cdot s$, con $r \neq 1, -1, a, -a$. Tomando valor absoluto, resulta $|a| = |r| \cdot |s|$. En virtud de la proposición anterior, $1 \leq |r| \leq |a|$. Pero, siendo $r \neq 1, -1, a, -a$, se cumple que $1 < |r| < |a|$. Finalmente, dado que r divide a a, $t = |r|$ es el factor que se buscaba. Esta proposición se utilizará repetidas veces. Con las mismas hipótesis, se sigue, además, la existencia de t_1 y $t_2 \in N$, tales que $1 < t_i < |a|$, $t_i \mid a$, $i = 1, 2$. (En el caso de $|a| = p^2$, p primo, $t_1 = t_2 = |p|$.)

2.8. **Teorema.** Todo entero distinto de 1 y -1 es divisible por un número primo.

Demostración. Razonemos por el absurdo. Supongamos que exista un entero $\neq 1, -1$ no divisible por ningún primo. Es claro que si t es tal entero, $|t|$ tampoco es divisible por ningún primo. Pero esto dice que hay enteros positivos $\neq 1$ no divisibles por ningún primo.

Por lo tanto, si llamamos H al conjunto de enteros positivos $\neq 1$ no divisibles por ningún primo, se sigue que $H \neq \emptyset$. Es claro que $1 \notin H$,

pues lo hemos excluido desde el principio. Por B. O. (Buena Ordenación) de N, se sigue que H posee un primer elemento g (g es el menor entero positivo $\neq 1$, no divisible por ningún primo).

Está claro que g no es primo, pues de otro modo $g|g$ y g sería divisible por un primo. Por lo tanto, se sigue de la proposición anterior que existe $k \in N$, $1 < k < g$ tal que $k|g$.

Pero $1 < k < g$ implica $k \notin H$ y, por lo tanto, k es divisible por un primo p. Como $k|g$, se concluye que $p|g$, lo que es una contradicción, que provino de suponer la existencia de enteros $\neq 1, -1$, no divisibles por primos. Se deja como ejercicio probar que todo entero distinto de $0, 1, -1$ es producto de primos.

2.9. Teorema. Existen infinitos primos en Z.

Demostración. Razonemos por el absurdo, suponiendo que haya a lo sumo un número finito de primos. Sean éstos $p_1, p_2, \ldots, p_k$. O sea, cualquier primo en Z es alguno de los p_i. Formemos el número entero

$$\Pi_{i=1}^{k} p_i = p_1 \cdot p_2 \ldots p_k$$

producto de todos los primos $p_1, p_2, \ldots, p_k$. Entonces $(\Pi_{i=1}^{k} p_i) + 1$ es es un número entero que no es ni 1 ni -1 (¿por qué?). Por lo tanto, es divisible por un primo q. O sea

$$\text{a)}\quad q\,|\,(\Pi_{i=1}^{k} p_i) + 1$$

pero como q es uno de los p_i

$$\text{b)}\quad q\,|\,\Pi_{i=1}^{k} p_i$$

De (a) y (b) se deduce que

$$q\,|\,1$$

por lo tanto, $q = 1$ o $q = -1$, lo que es absurdo (pues q es primo). Se concluye que hay infinitos primos en Z.

2. 10. Criterio para Encontrar Primos (Criba de Eratóstenes). Sea $a \in N$, $a \neq 1$, entonces a es divisible por un primo positivo. O sea, el conjunto de primos positivos que divide a a es no vacío, y posee, por lo tanto, un elemento mínimo que se denota por p.

Es así que $a = p \cdot x$. Si a no es primo, entonces $1 < x$ y, por el carácter mínimo de p, debe ser $p \leq x$. Por lo tanto, $p \leq x$ implica $p^2 \leq px = a$. Por lo tanto $p \leq \sqrt{a}$. Se ha probado, entonces, que un número entero $a > 1$ no es primo si, y sólo si, es divisible por un primo $p > 0$ tal que $p \leq \sqrt{a}$.

Este resultado se aplica para construir, para cada $M > 1$, una tabla de todos los primos positivos $\leq M$. Para ello es necesario conocer todos los primos $\leq \sqrt{M}$. Escritos los números a, $2 \leq a \leq M$, por cada primo positivo p, $p \leq \sqrt{M}$ se tachan todos sus múltiplos rp, $r \geq 2$, en esta enumeración. Los números que quedan sin tachar son exactamente los

primos positivos menores que M. En algún sentido se ha hecho un "tamizado" y este procedimiento se denomina la Criba de Eratóstenes. Por ejemplo, si $M = 49$, el esquema de la Criba es el siguiente:

2 3 ~~4~~ 5 ~~6~~ 7

~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13

~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19

~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ → {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47}

~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31

~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37

~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43

~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ ~~49~~

2. 11. Ejercicios

1. ¿Cuáles de los siguientes números son primos: 57, 91, 97, 113, 143, 187, 221, 223, 289, 589, 593, 607, 701, 943, 961, 1003, 1009?

2. Probar que si $n > 2$, existe al menos un primo p tal que $n < p < n!$

3. ¿Cuál es el primer primo en la sucesión natural de primos 2, 3, 5, 7, . . . , p_n, tal que $\prod_{i=1}^{n} p_i + 1$ no es un número primo?

4. Probar que todo número primo impar puede escribirse como diferencia de dos cuadrados consecutivos. Ejemplos: $3 = 2^2 - 1^2$, $5 = 3^2 - 2^2$, $7 = 4^2 - 3^2$.

5. Probar que todo primo de la forma $3k + 1$ es de la forma $6m + 1$.

6. Probar que hay infinitos primos de la forma $4m + 3$ y $6n + 5$. Mas difícil: hay infinitos primos de la forma $4k + 1$. **Nota.** Cabe mencionar el gran Teorema de Dirichlet (de 1837) que establece que si a y b son enteros positivos *coprimos*, la progresión aritmética $a + n \cdot b$, $n = 1, 2, 3, 4, \ldots$ contiene infinitos primos. Este teorema se suele llamar el teorema de los primos en progresión aritmética y de él se sigue que hay infinitos primos de la forma $3k + 1$, $5k + 7$, $6k + 13, \ldots$. Pregunta: ¿Habrá infinitos primos formados por sólo unos?

7. Probar que no hay progresiones aritméticas $a + nb$, $n = 1, 2, 3, \ldots$ que consisten *exclusivamente* en números primos.

8. Probar que 3, 5, 7 es la única terna de números primos positivos impares y consecutivos.

9. Probar que ningún número primo de la forma $4m + 3$ puede ser suma de dos cuadrados. Verificar que los primos menores de 100 de la forma $4m + 1$ *son* suma de dos cuadrados. **Nota.** Es posible probar

que un número primo impar es suma de dos cuadrados si, y sólo si, es de la forma $4m + 1$.

10. Sea p_n el n-simo primo. Probar que ninguno de los números $P_n = p_1 \cdot p_2 \ldots p_n + 1$ es un cuadrado perfecto.

11. Probar que para todo n existen n enteros consecutivos *compuestos*. (**Sugerencia.** Si $A = (n + 1)! + 2$, $A + 1$, $A + 2, \ldots$.)

12. Probar que no existe ningún polinomio $f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$ con coeficientes a_i enteros y de grado positivo (o sea $n \geq 1$) tal que $f(n)$ sea primo *para todo* n. A manera de compensación, verificar que el polinomio $f(X) = X^2 + X + 41$ satisface $f(n)$ primo para todo n, $1 \leq n \leq 39$. No se sabe si este polinomio da origen a infinitos primos.

13. Hallar el menor n tal que el polinomio $f(X) = X^2 + X + 17$ sea tal que $f(n)$ es compuesto. Hacer lo mismo con los polinomios $X^2 + 21X + 1$, $3X^2 + 3X + 23$ y $2X^2 + 29$.

14. i) Probar que si $n \in N$, entonces $2^n - 1$ es primo *sólo si* n es impar o $n = 2$.

ii) Probar que si $n \in N$, entonces $2^n - 1$ es primo *sólo si* n es primo.

15. i) Probar que si $n \in N$, entonces $2^n + 1$ es primo *sólo si* n es una potencia de 2.

ii) Sea $n \in N$. Se llama *número de Fermat* de orden n al número $F_n = 2^{2^n} + 1$. Si F_n es primo, se dice que es un primo de Fermat.

iii) Probar que si $n \neq m$, entonces F_n y F_m son coprimos. Esto permite otra demostración de la existencia de infinitos primos en Z.

Nota: Los únicos primos de Fermat que se conocen son $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ y $F_4 = 65637$. El número $F_5 = 2^{32} + 1$ *no es* primo. Euler probó que 641 es un divisor: $2^{32} + 1 = 4294967297 = 641 \times 6700417$. Una de las propiedades relevantes de los primos de Fermat se refiere a las construcciones geométricas con regla y compás: El polígono regular de n lados, n *primo*, es construible con regla y compás si, y sólo si, n es un primo de Fermat. Así el heptágono no es construible con regla y compás, pero sí lo es el heptadecágono (17 lados). La parte *si* del teorema anterior fue demostrada por Gauss y publicada en sus *Disquisitiones*. Sin embargo, en esa obra Gauss enuncia con toda generalidad la condición necesaria y suficiente para la construcción del polígono regular de n lados. La condición es que n debe ser una potencia de 2 por primos de Fermat distintos entre sí. El gran logro de Gauss se refiere, sin duda, a la construcción del polígono de 17 lados que ilumina completamente la situación general. Lo que es realmente interesante de señalar es el hecho que un problema *geométrico* tenga una solución totalmente *aritmética*.

16. Probar inductivamente que si p_n es el n-simo primo, entonces $p_n \leq 2^{2^{n-1}}$. Este resultado puede mejorarse mucho si se recurre al llamado *Postulado de Bertrand* enunciado por Bertrand y probado por Tchebychef en 1850, que establece que si $n > 1$, entonces existe siem-

pre un primo p que satisface $n < p < 2n$. A partir de este postulado, probar que $p_n < 2^n$, $n > 1$.

2. 12. Complemento

1. Un problema famoso relativo a números primos, de carácter distinto al de los problemas usuales, es la llamada conjetura de Goldbach. Christian Goldbach (1690- 1764), matemático alemán que ocupó una posición importante en la Academia de Ciencias de San Petersburgo, mantuvo correspondencia con Euler durante muchos años. En una carta enviada por éste a Euler en Berlín, hacía la conjetura que todo número par mayor que 4 era suma de dos primos impares. Por ejemplo: $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7$, $12 = 5 + 7 \ldots$. Hay sobrada evidencia numérica sobre la posible veracidad de esta conjetura, sin embargo sigue siendo en la actualidad un problema no resuelto aún. Cabe notar que si la conjetura de Goldbach es cierta, entonces todo número impar mayor que 8 es suma de tres primos impares.

En 1934, el matemático ruso I. M. Vinogradov demostró la existencia de un entero n_0 con la propiedad que todo número impar mayor que n_0 es expresable como la suma de tres primos impares. La conjetura de Goldbach constituye un problema de la *teoría aditiva de números*. Esta teoría tiene por objeto determinar, dado un conjunto S de números, ¿qué números enteros son expresables como suma de un número fijo de elementos de S? Por ejemplo, en la conjetura de Goldbach, S es el conjunto de primos positivos o primos positivos impares. Otro resultado de la teoría aditiva de números es el célebre *Teorema de Lagrange*, que dice que todo entero positivo es suma de cuatro cuadrados en Z.

3

ALGORITMO DE DIVISION EN Z

3.1. Teorema. **Existencia del Algoritmo de División (AD) en Z.** Sean a y $b \in Z$, $b > 0$. Entonces:

AD1) Existen enteros q y r tales que

$$a = b \cdot q + r, \text{ con } 0 \le r < b.$$

AD2) Si $a = b \cdot q + r$, con $0 \le r < b$, y

$$a = b \cdot q' + r', \text{ con } 0 \le r' < b,$$

entonces $q = q'$ y $r = r'$.

q y r se denominan, respectivamente, el *cociente* y el *resto* de la división de a por b. Parte AD1) asegura la existencia del cociente y del resto. Parte AD2) establece la unicidad de los mismos.

Demostración. AD1) Sea $N_0 = N \cup \{0\}$. N_0 no es otra cosa que la "semirrecta entera" a la derecha, de origen 0, o más corrientemente, es el conjunto de números naturales con el 0 agregado. N_0 es un conjunto bien ordenado.

Sea $L = \{a - k \cdot b \mid k \in Z\}$ la totalidad de enteros de la forma $a - k \cdot b$ para algún $k \in Z$.

Como ejemplo, se indican casos de números pertenecientes a L:

$$a = a - 0 \cdot b \in L,$$

$$a - b = a - 1 \cdot b \in L,$$

$$a + b = a - (-1) \cdot b \in L.$$

$0 \in L$ si, y sólo si, $b \mid a$,

$L = Z$ si, y sólo si, $b = 1$.

Se afirma que

$$L \cap N_0 \neq \emptyset \qquad [*]$$

En efecto:

si $0 \le a$, entonces $a - 0 \cdot b = a \in L \cap N_0$,

si $a < 0$, entonces $0 < -a$, y como $0 < b$ es $0 \le b - 1$.

Por lo tanto $0 \leq (-a) \cdot b - (-a) = a - a \cdot b \in L \cap N_0$. Queda probada nuestra afirmación [*]. Puesto que $L \cap N_0 \subset N_0$ y N_0 es bien ordenado, $L \cap N_0$ posee un elemento minimal r. Las propiedades de r son:

$$r = a - q \cdot b \text{ para algún } q \in Z,$$

$$0 \leq r \in N_0, \text{ o sea } a = q \cdot b + r, \ 0 \leq r.$$

Quedaría por ver que $r < b$. Razonemos por el absurdo, suponiendo $b \leq r$ es $r = b + (r - b)$. Entonces

$$a = q \cdot b + r = (q + 1) \cdot b + (r - b)$$

$$b \leq r \text{ implica } r - b \geq 0$$

con lo que $r - b \in L \cap N_0$. Debe ser, pues, $r \leq r - b$, o sea $b \leq 0$, lo que es absurdo. Se sigue que $r < b$ y AD1) queda probado.

AD2) Sean:

$$a = q \cdot b + r, \ 0 \leq r < b;$$

$$a = q' \cdot b + r', \ 0 \leq r' < b.$$

Por lo tanto, $(q - q') \cdot b = r' - r$ y tomando el valor absoluto

$$|q - q'| \cdot b = |r' - r|$$

Si $q \neq q'$, $|q - q'| > 0$, entonces $|q - q'| \geq 1$, por lo tanto

$$|r' - r| = |q - q'| \cdot b \geq b \qquad [**]$$

Por otra parte, $r \geq 0$ implica $-r \leq 0$ y así $r' - r \leq r' < b$

$$r < b \leq b + r' \text{ implica } -b < r' - r.$$

Entonces $-b < r' - r < b$, es decir $|r' - r| < b$, lo cual contradice [**]. Debe ser, pues, $|q - q'| = 0$, con lo que $q = q'$ y $r = r'$. El teorema ha quedado demostrado.

3.2. Ejemplos

1. $a = 4231$, $b = 7$

   $4231 = 7 \times 604 + 3$, $q = 604$, $r = 3$

2. $a = -4231$, $b = 7$

   $-4231 = 7 \cdot (-604) + (-3) = 7 \cdot (-605) + 4$

   $q = -605$, $r = 4$.

3.3. Corolario. Sean a y $b \in Z$, $b \neq 0$. Existen, entonces, únicos enteros q y r tales que $a = b \cdot q + r$, con $0 \leq r < |b|$.

Demostración. Sean q y r tales que $a = |b| \cdot q + r$, con $0 \leq r < |b|$. Entonces, si $b > 0$ no hay nada que probar. Si $b < 0$, entonces $|b| = -b$ y puede escribirse

$$a = b \cdot (-q) + r, \quad \text{con } 0 \leq r < |b|.$$

La unicidad es inmediata.

3.4. Corolario y Definición. Sean a y b enteros, $b \neq 0$. Sean q y r tales que $a = q \cdot b + r$, $0 \leq r < |b|$. Entonces $b|a$ si, y sólo si, $r = 0$.

Demostración. Si $r = 0$, es claro que $b|a$. Recíprocamente, sea $a = q' \cdot b$. Se tiene:

$$a = q \cdot b + r, \; 0 \leq r < |b| \text{ y}$$

$$a = q' \cdot b + 0$$

Por unicidad debe ser $r = 0$. Queda demostrado el corolario.

Definición. Un número entero m se dice *par*, si $2|m$, e *impar*, si $2\nmid m$.

3.5. Ejercicios

1. Probar que ningún $n \in N$ es par e impar a la vez.

2. Probar que para todo $n \in N$, n es par si, y sólo si, n^2 es par.

3. Probar que $n \in N$ es par si, y sólo si, para todo $j \in N$, n^j es par.

4. ¿Cuáles de los siguientes números enteros son pares, $n \in N$?

i) $3 \cdot n^2 + 1$,

ii) $n \cdot (n + 1)$,

iii) $(n - 1) \cdot (n + 1)$,

iv) $n^3 - n$,

v) $(-1)^{n-1} \cdot 3 + (-1)^n \cdot 3$,

vi) $n \cdot (3n + 1)$,

vii) $(n + 1) \cdot (5n + 2)$.

(En los casos en que la respuesta sea negativa, indicar si hay valores de n para los cuales los números anteriores son pares).

5. Probar que hay dos únicos primos pares.

6. Probar que todo primo impar tiene una de las formas: $4m + 1$ ó $4m + 3$, con $m \in Z$.

7. Probar que todo primo $\neq \pm 2, \pm 3$ es de la forma $6m - 1$ o $6m + 1$, con $m \in Z$.

8. Probar que todo primo mayor que 5 es de la forma $30m + n$, con $n = 1, 7, 11, 13, 17, 19, 23$ ó 29.

9. Probar que la suma de dos cuadrados impares nunca es un cuadrado.

10. Probar que todo entero de la forma $4m + 3$ tiene un número impar de factores de la forma $4m - 1$.

11. Probar que si t es un entero mayor que 1, el número $t^{4m} + t^{2m} + 1$ nunca es primo. (**Sugerencia.** Notar la identidad $t^4 + t^2 + 1 = (t^2 + t + 1)(t^2 - t + 1)$).

12. Probar que el cubo de todo número entero es la diferencia de dos cuadrados enteros. (**Sugerencia.** $[\frac{n(n+1)}{2}]^2 = 1^3 + 2^3 + \ldots + n^3$).

3.6. **Ejemplos**

1. El resto de la división de un número por 4 es 3 y el resto de la división del mismo número por 9 es 5. Encontrar el resto de la división del número por 36.

Solución. Se tiene $a \in N$, tal que

$$a = 4 \cdot q + 3$$

$$a = 9 \cdot k + 5$$

Se trata de hallar el resto de la división de a por 36, y se escribe

$$4 \cdot q + 3 = 9 \cdot k + 5$$

$$4 \cdot q = 9 \cdot k + 2$$

$$4 \cdot (q - 2 \cdot k) = k + 2$$

con lo que $4 | k + 2$, o sea $k + 2 = 4m$, luego $k = 4 \cdot m - 2$ y así

$$a = 9 \cdot (4 \cdot m - 2) + 5 = 36 \cdot m - 18 + 5 =$$

$$= 36m - 13 = 36(m - 1) + 23$$

la respuesta es 23.

2. Se sabe que el resto de la división de 748 por un número n positivo es 20 y el resto de la división de 1229 por n es 33. Se pide hallar n. Se tiene

$$748 = n \cdot x + 20, \quad \text{o sea} \quad n | 728$$

$$1229 = n \cdot y + 33, \quad \text{o sea} \quad n | 1196$$

Se tiene además

$$n \cdot (y - x) = 1229 - 748 - 33 + 20 = 481 - 13 = 468$$

o sea $n|468 = 4 \times 9 \times 13$.

La condición $n|728 = 2^3 \times 91$ implica que $3 \nmid n$. Además, $n > 33$. La única posibilidad para n es $52 = 4 \cdot 13$ y ésta es la respuesta al ejercicio. (Observe el lector que se ha utilizado el T. F. A.)

3. Denotemos por $r_b(m)$ el resto de la división de m por b. Probar las relaciones siguientes:

$$r_b(m + n) = r_b(r_b(m) + r_b(n))$$

$$r_b(m \cdot n) = r_b(r_b(m) \cdot r_b(n))$$

Por ejemplo, si 5 es el resto de la división de un número m por 9, entonces:

$$r_9(m^2) = r_9(5^2) = 7, \quad r_9(3m + 41) =$$

$$= r_9(3 \cdot 5 + 5) = 2.$$

4. Calcular el resto de la división de $n = (34210987654345654321\,34567)^2$ por 9. Se sabe que el resto de la división del número entre paréntesis en la división por 9 se obtiene sumando las cifras y reduciendo módulo 9. La suma reducida módulo 9 es 8 y $n = 9 \cdot k + 8$. Por lo tanto, el número $(34 \ldots 67)^2$ tiene el mismo resto en la división por 9 que el número $8^2 = 64$, a saber 1. Ese es el resultado. 29

5. Calculemos todos los restos posibles de la división de un cuadrado por 7. O sea, calcular los restos de n^2 en la división por 7. Para ello se escribe

$$n = 7 \cdot k + r, \quad \text{donde } r = 0, 1, 2, 3, 4, 5, 6$$

Puesto que

$$n^2 = 7 \cdot k' + r^2 \quad (\text{con } k' = 7 \cdot k^2 + 2kr)$$

el problema se reduce a calcular los restos de 0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2. Estos son, respectivamente, 0, 1, 4, 2, 2, 4, 1.

Veamos una consecuencia: sean m y n enteros. Entonces

$$7|m^2 + n^2 \Leftrightarrow 7|m \text{ y } 7|n$$

La parte $\Leftarrow$ es trivial. Para la otra implicación basta observar que la suma de dos restos cuadráticos 0, 1, 2, 4 puede producir un múltiplo de 7 en el único caso de resto 0, o sea 0 + 0, que dice bien que m^2 y n^2 son divisibles por 7 y, por lo tanto lo son m y n, dado que al analizar restos se observa que $7|m^2$ si, y sólo si, $7|m$.

6. Calculemos todos los restos posibles de la división de un cuadrado por 13. Los restos de la división por 13 son:

0 1 2 3 4 5 6 7 8 9 10 11 12

y los de sus cuadrados

0 1 4 9 3 12 10 10 12 3 9 4 1

El primo 13 no goza de la propiedad que goza el 7 (Ejemplo 6):

$$13 \mid 5^2 + 1^2, \text{ pero } 13 \nmid 5 \text{ y } 13 \nmid 1$$

Hallar los restos cúbicos módulo 13, o sea los posibles restos de la división de n^3 por 13.

7. Calculemos los restos en la división por 7 de n, n^2, n^3, ... Los cálculos se disponen según la tabla siguiente:

n	=	0	1	2	3	4	5	6
n^2	=	0	1	4	2	2	4	1
n^3	=	0	1	1	6	1	6	6
n^4	=	0	1	2	4	4	2	1
n^5	=	0	1	4	5	2	3	6
n^6	=	0	1	1	1	1	1	1
n^7	=	0	1	2	3	4	5	6

Se observa que los restos "periódicos" se repiten con "período" 7:

$$\text{resto } x = \text{resto } x^7 \text{ y resto } x^m = \text{resto } x^{m+7k}$$

Nótese, además, que si el resto $x \neq 0$, entonces el resto $x^6 = 1$. Como aplicación, calcular el resto de la división por 7 de 9999^{9999} El resto de la división de 9999 por 7 es 3. Ahora

$$\text{resto}(9999^{9999}) = \text{resto}(3^{9999}) = \text{resto}(3^{6 \cdot 1666} \cdot 3^3) = \text{resto } 3^3 = 6$$

Nótese que: $7 \mid a^3 + b^3 + c^3 \Rightarrow 7 \mid abc$

$$7 \mid \textstyle\sum_1^n a_i^6 \Rightarrow 7 \mid \Pi a_i, \text{ o } 7 \mid n$$

$$7 \mid a^2 + b^2 \Rightarrow 7 \mid a \text{ y } 7 \mid b$$

$$7 \mid a^4 + b^4 \Rightarrow 7 \mid a \text{ y } 7 \mid b$$

$$7 \mid a^2 + 2b^2 \Rightarrow 7 \mid a \text{ y } 7 \mid b$$

$$7 \mid a^2 + 4b^2 \Rightarrow 7 \mid a \text{ y } 7 \mid b$$

8. Sea $a \in N$, $a > 1$. Sean n, $m \in N$. Se afirma que $a^n - 1 | a^m - 1$ si, y sólo si, $n | m$. A manera de ejemplo probemos esta afirmación. Recordemos la conocida identidad algebraica

$$a^r - b^r = (a - b) \cdot (a^{r-1} + b \cdot a^{r-2} + \ldots + b^{r-1})$$

cuya demostración se hace por inducción. Si n divide a m se sigue inmediatamente de esta identidad que $a^n - 1$ divide a $a^m - 1$.

Veamos la recíproca: Si $a^n - 1 | a^m - 1$, entonces $n | m$.

$$a^n - 1 | a^m - 1 \Rightarrow a^n - 1 \leq a^m - 1 \Rightarrow n \leq m \Rightarrow m = nq + r \text{ y } q \geq 0 \Rightarrow nq \geq 0$$

Además, $0 \leq r < n$. Si $r = 0$, $n | m$ y la afirmación está probada.

Si $r > 0$

$$a^m - 1 = (a^{n \cdot q} - 1) \cdot a^r + (a^r - 1)$$

Por lo tanto

$$a^n - 1 | a^m - 1 \text{ y } a^n - 1 | a^{n \cdot q} - 1 \text{ (caso anterior)}$$

implican

$$a^n - 1 | a^r - 1 \qquad [*]$$

Ahora, $0 < r < n$ y $1 < a$ implican $1 < a^r < a^n$, o sea $0 < a^r - 1 < a^n - 1$, lo cual contradice [*]. Por lo tanto, es $r = 0$ y así $n | m$.

9. **Aplicación.** ¿Qué día de la semana fue el 25 de febrero de 1778? Para contestar esta pregunta es necesario recordar que en nuestro calendario un año normal consta de 52 semanas y 1 día, o sea 365 días. Un año bisiesto consta de un día más, agregado al mes de febrero, o sea consta de 366 días. Un año que no es secular (o sea que no corresponde a un siglo) es bisiesto si, y sólo si, es divisible por 4. Los años seculares, tales como 1600, 1700, 1800, 1900,... son bisiestos si, y sólo si, son divisibles por 400. Por consiguiente, los años 1600 y 2000 son bisiestos, pero no lo son los años 1700, 1800 y 1900.

La observación fundamental para determinar en qué día de la semana cayó una fecha dada es que dos fechas dadas caen en el mismo día de la semana si, y sólo si, el número de días del intervalo que forman esas dos fechas tiene resto 1 en la división por 7. Por ejemplo, lo que todos observamos en el calendario:

Lunes 1, Lunes 8, Lunes 15, Lunes 22, Lunes 29

Así, por ejemplo, si el 1 de enero fue sábado y el año no es bisiesto, del 1 de enero al 31 de diciembre hay $365 = 52 \cdot 7 + 1$. Por lo tanto, ambas fechas caen el mismo día de la semana. Si el año fuera bisiesto sería $366 = 52 \cdot 7 + 2$, por lo tanto el 31 de diciembre caería el día siguiente de la semana al correspondiente al primero de enero.

Con esta digresión es posible calcular el día de la semana que le correspondió al 25 de febrero de 1778. La información básica se obtiene de un calendario de 1984 que tenemos a mano.

i) Años transcurridos de 1778 a 1984: 1984 - 1778 = 206 años.

ii) Años bisiestos intermedios. Estos van de 1780 a 1980, o sea 1980 - 1780 = 200. Pero 1800 y 1900 no fueron bisiestos. Por lo tanto, el número de años bisiestos intermedios fue $(\frac{200}{4} + 1) - 2 = 49$.

iii) Del 25 de febrero de 1778 al 25 de febrero de 1984 transcurrieron 206 años + 1 día.

Por lo tanto el número total de días fue:

$$206 \cdot 365 + 49 + 1 = 75240 = 10748 \cdot 7 + 4$$

Dado que el 25 de febrero de 1984 fue sábado se tiene que el 25 de febrero de 1778 fue: sábado-viernes-jueves-*miércoles*. Fue entonces miércoles.

Hallemos qué día de la semana nació Gauss si sabemos que la fecha fue el 30 de abril de 1777. El 30 de abril de 1984 fue lunes.

Años transcurridos: 1984 - 1777 = 207.

Años bisiestos: 1984 - 1780 = 204, o sea $(\frac{204}{4} + 1) - 2 = 50$.

Días transcurridos: $207 \cdot 365 + 50 + 1 = 75606 = 10800 \cdot 7 + 6$.

Por lo tanto, el 30 de abril de 1778 fue: lunes-domingo-sábado-viernes-jueves-*miércoles*. Fue entonces un día miércoles.

Se deja a cargo del lector determinar qué día de la semana:

i) murió el Gen. San Martín (agosto 17, 1850) (Respuesta: sábado),

ii) murió Gauss (febrero 23, 1855) (Respuesta: viernes),

iii) nació Euler (abril 15, 1707) (Respuesta: viernes),

iv) murió Euler (septiembre 18, 1783) (Respuesta: jueves), y

v) fue el día D: 6-6-44 (Respuesta: martes).

3.7. **Ejercicios**

1. Efectuar la división de a por b en los casos siguientes:

i) $a = 957$, $b = 12$	iv) $a = 2466$, $b = -11$
ii) $a = 127$, $b = 99$	v) $a = 132$, $b = -89$
iii) $a = -1356$, $b = -71$	vi) $a = -98$, $b = -73$

2. Dado $m \in Z$, $m \neq 0$, hallar los restos posibles de m^2 y m^3 en la división por 3, 4, 5, 7, 8, 11.

3. Sean a y b enteros, $b > 0$. Determinar la división de $b - a$ por b, a partir de la división de a por b.

4. Sean a y b enteros, $b \neq 0$. Si $a - b = 175$ y la división de a por b tiene cociente 15 y resto 7, hallar a y b.

5. Probar que todo entero impar, que no es múltiplo de 3, es de la forma $6m \pm 1$, m entero.

6. ¿Qué números $n \in N$ tienen la propiedad: i) divididos por a, poseen el mismo cociente y resto, y ii) divididos por 9, poseen por cociente el complemento a 9 del resto?

7. Sean a y b enteros. Entonces $a^3 - b^3$ es divisible por 11 si, y sólo si, $a - b$ es divisible por 11. (**Sugerencia.** Estudie, dado $m \in Z$, $m \neq 0$, los restos posibles de m^3 en términos de los restos de m.)

8. Probar que si a y b son enteros, entonces $a^2 + b^2$ es divisible por 3 si, y sólo si, a y b son divisibles por 3. A partir de este resultado dar una demostración de la irracionalidad de $\sqrt{2}$.

9. Probar que: i) la suma de cuadrados de tres números no divisibles por 3 es un múltiplo de 3, y ii) la diferencia de cuadrados de dos números no divisibles por 3 es un múltiplo de 3.

10. Dada una sucesión $a_1, \ldots, a_n$ de enteros, probar que siempre es posible extraer una subsucesión cuya suma es divisible por n. (**Sugerencia.** Considere los n números a_1, $a_1 + a_2$, $a_1 + a_2 + a_3, \ldots$, $a_1 + a_2 + \ldots + a_n$ y analice los restos en la división por n.)

11. Sea A un número escrito en forma decimal, forme los números $A_1 = A$, $A_2 = AA$ y $A_3 = AAA$, ... repitiendo las cifras de A. (Por ejemplo, si $A = 13$, $A_2 = 1313$, $A_3 = 131313$). Probar que si m es un entero, coprimo con 10, entonces m divide a infinitos números A_n.

12. Sean a, b y c enteros tales que $a^2 + b^2 = c^2$. Probar que:

i) a o b es par,

ii) a o b es divisible por 3,

iii) a o b es divisible por 4,

iv) a o b o c es divisible por 5.

v) Hallar todas las ternas coprimas a, b, c, $\in N$, tales que $a^2 + b^2 = c^2$. (**Respuesta.** $a = x^2 - y^2$, $b = 2xy$, $c = x^2 + y^2$, donde x e y recorren todos los enteros que satisfacen: $0 < y < x$, $(x, y) = 1$, x e y son de distinta paridad.)

13. Probar que ningún entero positivo de la forma $8k + 7$ puede expresarse como la suma de tres cuadrados en Z. (**Nota.** Gauss prueba en sus *Disquisitiones* que la condición necesaria y suficiente para que un entero positivo n sea la suma de tres cuadrados en Z es que n *no sea* de la forma $4^a \cdot (8b + 7)$, con a y b en Z. Un célebre teorema de Lagrange establece que todo entero positivo es suma de cuatro cuadrados en Z. Probar a partir del teorema de Gauss, el teorema de Lagrange.)

14. Sean p y q primos distintos, ambos mayores que 3. Probar que si $p - q$ es una potencia de 2, entonces $p + q$ es divisible por 3.

15. Sean $f(X)$ un polinomio con coeficientes enteros y $k \in N$, tales que k no divide a $f(t)$ para todo $t = 1, \ldots, k$. Probar que $f(X)$ no posee ninguna raíz entera. (**Sugerencia.** Sea a en Z con $f(a) = 0$. Existe entonces un polinomio $g(X)$ con coeficientes enteros tal que $f(X) = (X - a) \cdot g(X)$. Sea j, $1 \leq j \leq k$ tal que $a = k \cdot q + j$. Como $k|(a - j)$, se sigue que $k|f(j)$ es una contradicción.)

16. Sean a y b enteros positivos con las propiedades:

$$a|b^2, \; b^2|a^3, \; a^3|b^4, \; b^4|a^5, \ldots$$

Probar que $a = b$. (**Sugerencia.** Sea $a < b$. Se tiene que $(\frac{a}{b})^n$ tiende a cero cuando n tiende a infinito. Deducir una contradicción.)

4

MAXIMO COMUN DIVISOR

Sean a y b enteros, $(a, b) \neq (0, 0)$ (o sea no simultáneamente nulos).

4.1. Teorema. Existe $d \in N$ con las siguientes propiedades:

i) $d|a$ y $d|b$, y

ii) existen enteros u y v tales que $d = u \cdot a + v \cdot b$.

Demostración. Vamos a suponer, sin pérdida de generalidad, que b es positivo, o sea $b \in N$. Para demostrar nuestra afirmación se procederá inductivamente en b. Así, si $b = 1$, $d = 1$ tiene las propiedades pedidas, pues

$$1|a \text{ y } 1|b$$

$$1 = 1 \cdot a + (1 - a) \cdot 1 \quad (\text{o sea } u = 1,\ v = 1 - a)$$

Sea, entonces, $1 < b$. Supondremos el teorema válido para todos los enteros positivos menores que b, cualquiera que sea a. La tarea consistirá en probar que el teorema es cierto para b. En virtud del algoritmo de división se escribe

$$a = q \cdot b + r, \quad \text{con } 0 \leq r < b \qquad [*]$$

Si $r = 0$, entonces $b|a$, y basta tomar $d = b$ para probar el teorema, dado que si $d = b$

$$d|a \text{ y } d|b$$

$$d = b = 0 \cdot a + 1 \cdot b \qquad (u = 0 \text{ y } v = 1)$$

Si $r \neq 0$, entonces $1 \leq r < b$. Por la hipótesis inductiva aplicada a r existe $d \in N$ tal que

$$d|b \text{ y } d|r \qquad [**]$$

y existen enteros x e y tales que $d = x \cdot b + y \cdot r$

Notemos que de [*] y [**]

$$d|b \text{ y } d|r \text{ implican } d|a$$

Por lo tanto $d|a$ y $d|b$, y además

$$d = x \cdot b + y \cdot r = x \cdot b + y \cdot (a - q \cdot b) =$$
$$= xb - yqb + ya = ya + (x - yq) \cdot b$$

Todo esto dice que el teorema es válido para b. En virtud del principio de inducción, el teorema es válido para todo b y a. El teorema queda demostrado.

4.2. Teorema. El d de 4.1. es único, o sea si $d' \in N$ satisface:

i) $d'|a$ y $d'|b$, y

ii) existen enteros u' y v' tales que $d' = u'a + v'b$, entonces $d = d'$.

Demostración

$d|a$ y $d|b$, y $d' = u'a + v'b$ implican $d|d'$, luego $d \leq d'$

$d'|a$ y $d'|b$, y $d = u \cdot a + v \cdot b$ implican $d'|d$, luego $d' \leq d$,

por lo tanto $d = d'$.

4.3. Definición y Ejemplos

1. Dados $a, b \in Z$ $(a, b) \neq (0, 0)$, entonces el único entero positivo asociado al par a, b, según 4.1., se denomina *máximo común divisor* (m. c. d.) de a y b y se denota por (a, b).

2. Se define $(0, 0) = 0$.

3. Es claro que si a y b son enteros, entonces $(a, b) = (b, a) = (-a, b) = (a, -b) = (-a, -b)$.

4. i) Si $a \neq 0$, $(a, b) = |a|$ si, y sólo si, $a|b$.

   ii) Si $c|a$ y $c|b$, entonces $c|(a, b)$.

5. Determinemos d en la situación $b = 45$, $a = 84$. La demostración del teorema precedente sugiere la forma de encontrar d. La idea es usar divisiones sucesivas

$$\begin{aligned} 84 &= 45 \cdot 1 + 39 \\ 45 &= 39 \cdot 1 + 6 \\ 39 &= 6 \cdot 6 + 3 \\ 6 &= 3 \cdot 2 \end{aligned}$$

recuérdese que en el teorema anterior el d asociado a a y b era el mismo que el asociado a b y r, es decir $(a, b) = (b, r)$, por lo tanto

$$(84, 45) = (45, 39) = (39, 6) = (6, 3) = 3, \text{ pues } 3|6$$

Veamos cómo se encuentran los u y v. Despejando 3 en términos de 84 y 45 resulta

$$\begin{aligned} 3 &= 39 - 6 \cdot 6 = 39 - 6 \cdot (45 - 39 \cdot 1) = 7 \cdot 39 - 6 \cdot 45 = \\ &= 7 \cdot (84 - 45 \cdot 1) - 6 \cdot 45 = 7 \cdot 84 - 13 \cdot 45 = \\ &= 7 \cdot 84 + (-13) \cdot 45 \end{aligned}$$

6. El mismo problema con -84 y 45. Del ejemplo anterior se tiene:

$$d = 3 = 7 \cdot 84 + (-13) \cdot 45 = (-7) \cdot (-84) + (-13) \cdot 45$$

$$3 = (84, 45) = (-84, 45)$$

7. El mismo problema con 84, -45

$$d = 3 = 7 \cdot 84 + (-13) \cdot 45 = 7 \cdot 84 + 13 \cdot (-45)$$

$$3 = (84, 45) = (84, -45)$$

8. $(4, 6) = 2 = (-1) \cdot 4 + 1 \cdot 6$

$(0, -5) = 5 = 1 \cdot 0 + (-1) \cdot (-5)$

$(-4, -6) = 2 = 1 \cdot (-4) + (-1) \cdot (-6)$

$(924, 156) = 12 = (-1) \cdot 924 + 6 \cdot 156$

$(17, 23) = 1 = (-4) \cdot 17 + 23 \cdot 3$

$(524, 634) = 2 = (-98) \cdot 524 + 81 \cdot 634$

$(943, 414) = 23 = (-7) \cdot 943 + 16 \cdot 414$

9. **Ejemplo.** Calculemos en detalle $(943, 414) = 23$. Por el algoritmo de división se tiene:

$$943 = 414 \cdot 2 + 115$$

$$414 = 115 \cdot 3 + 69$$

$$115 = 69 \cdot 1 + 46$$

$$69 = 46 \cdot 1 + 23$$

$$46 = 23 \cdot 2$$

Escribamos ahora $a = 943$ y $b = 414$. De las relaciones precedentes se sigue:

$$115 = a - 2b$$

$$69 = b - 3 \cdot (a - 2b) = 7b - 3a$$

$$46 = a - 2b - (7b - 3a) = -9b + 4a$$

$$23 = 7b - 3a - (-9b + 4a) = 16b - 7a = 16 \cdot 414 + (-7) \cdot 943$$

4.4. Relación del Algoritmo de Euclides con los Desarrollos en Fracciones Continuadas o en Cadena de Fracciones

El algoritmo de Euclides está íntimamente ligado al proceso de formar fracciones continuadas, o sea expresiones del tipo

$$\cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{\ddots \, a_{n-1} + \cfrac{b_n}{a_n}}}}$$

con $a_i, \ b_i \in N$.

Sea, en efecto, el algoritmo de división aplicado reiteradamente para obtener el máximo común divisor:

$$\begin{aligned}
a &= q_1 b + r_2, \quad 0 < r_2 < b \\
b &= q_2 r_2 + r_3, \quad 0 < r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4, \quad 0 < r_4 < r_3 \\
&\dots \qquad\qquad \dots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n
\end{aligned}$$

Estas expresiones pueden escribirse como sigue:

$$\begin{aligned}
\frac{a}{b} &= q_1 + \frac{r_2}{b}, \ \frac{r_2}{b} < 1 \\
\frac{b}{r_2} &= q_2 + \frac{r_3}{r_2}, \ \frac{r_3}{r_2} < 1 \\
\frac{r_2}{r_3} &= q_3 + \frac{r_4}{r_3}, \ \frac{r_4}{r_3} < 1 \\
&\dots\dots \qquad \dots
\end{aligned}$$

Por lo tanto

$$\frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \cfrac{1}{\cfrac{b}{r_2}}$$

$$= q_1 + \cfrac{1}{q_2 + \cfrac{r_3}{r_2}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cfrac{r_2}{r_3}}} = \dots$$

Se obtiene la expresión siguiente de $\frac{a}{b}$ como fracción continuada:

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

Por ejemplo, a partir de

$$943 = 414 \cdot 2 + 115$$
$$414 = 115 \cdot 3 + 69$$
$$115 = 69 \cdot 1 + 46$$
$$69 = 46 \cdot 1 + 23$$
$$46 = 23 \cdot 2$$

se obtiene la siguiente expresión de $\frac{943}{414}$ como fracción continuada

$$\frac{943}{414} = 2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}$$

Cada fracción parcial

$$2, \quad 2 + \frac{1}{3}, \quad 2 + \cfrac{1}{3 + \cfrac{1}{1}}, \quad 2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1}}}$$

conduce a una aproximación de $\frac{943}{414}$.

El hecho relevante es que la última fracción indicada (que sería la penúltima en la construcción precedente) da lo siguiente. Operando vemos que

$$2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1}}} = 2 + \frac{2}{7} = \frac{16}{7}$$

$$\frac{943}{414} - \frac{16}{7} = \frac{943 \cdot 7 - 414 \cdot 16}{414 \cdot 7} = \frac{-23}{414 \cdot 7}$$

que permite expresar $23 = (943, 414) = 943 \cdot -7 + 414 \cdot 16$.

Volviendo a la discusión inicial, consideremos las fracciones parciales

$$\delta_1 = q_1$$
$$\delta_2 = q_1 + \frac{1}{q_2}$$
$$\delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}$$

Es claro que $\delta_n = \frac{a}{b}$.

Cada expresión δ_k $(k = 1, \ldots, n)$ se denomina una *convergente de orden* k de $\frac{a}{b}$. Es fácil ver que las distintas convergentes de $\frac{a}{b}$ aproximan a esta fracción en la forma

$$\delta_1 < \delta_3 < \ldots \delta_{2k-1} < \ldots < \frac{a}{b} < \delta_{2k} < \ldots \delta_4 < \delta_2$$

Escribamos como fracción irreductible:

$$\frac{P_k}{Q_k} = \delta_k \qquad 1 \leq k \leq n$$

y consideremos la ley de formación de numerador y denominador. Se tiene

$$\delta_1 = \frac{P_1}{Q_1} = \frac{q_1}{1}, \; P_1 = q_1, \; Q_1 = 1$$

$$\delta_2 = \frac{P_2}{Q_2} = q_1 + \frac{1}{q_2} = \frac{q_1 q_2 + 1}{q_2}, \; P_2 = q_1 q_2 + 1, \quad Q_2 = q_2$$

$$\delta_3 = \frac{P_3}{Q_3} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} = \frac{q_1 q_2 q_3 + q_1 + q_3}{q_2 q_3 + 1}$$

$$P_3 = q_1 q_2 q_3 + q_1 + q_3 = q_3 P_2 + P_1$$

$$Q_3 = q_2 q_3 + 1 = q_3 q_2 + Q_1$$

Se puede ver inductivamente que para todo $k \geq 3$ se satisface

$$P_k = q_k P_{k-1} + P_{k-2}, \quad Q_k = q_k Q_{k-1} + Q_{k-2}$$

Las diferencias $\delta_k - \delta_{k-1}$ satisfacen la relación

$$\delta_k - \delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k Q_{k-1} - P_{k-1} Q_k}{Q_k Q_{k-1}} = \frac{(-1)^k}{Q_k Q_{k-1}} \qquad [*]$$

En efecto, se tiene

$$P_k Q_{k-1} - P_{k-1} Q_k = (q_k P_{k-1} + P_{k-2}) Q_{k-1} - P_{k-1}(q_k Q_{k-1} + Q_{k-2})$$

$$= -(P_{k-1} Q_{k-2} - P_{k-2} Q_{k-1})$$

y repitiendo el razonamiento

$$= (-1)^2 (P_{k-2} Q_{k-3} - P_{k-3} Q_{k-2})$$

$$\cdots\cdots\cdots$$

$$= (-1)^{k-2} (P_2 Q_1 - P_1 Q_2)$$

$$= (-1)^{k-2}(q_1q_2 + 1 - q_1q_2) = (-1)^{k-2} = (-1)^k$$

Se sigue la validez de [*].

Entonces

$$\frac{a}{b} - \delta_{n-1} = \frac{(-1)^n}{bQ_{n-1}}$$

O sea

$$a \cdot Q_{n-1} - b \cdot P_{n-1} = (-1)^n$$

En consecuencia, se dispone de un método para calcular la relación $ax + by = 1$ y, por lo tanto, de resolver la ecuación $ax + by = c$. Una forma práctica de proceder es utilizar el siguiente diagrama:

		q_1	q_2	q_3		q_{n-2}	q_{n-1}	q_n
0	1	$P_1 \overset{+}{\longleftarrow}$	P_2	P_3	...	P_{n-2}	P_{n-1}	P_n
1	0	$Q_1 \overset{+}{\longleftarrow}$	Q_2	Q_3	...	Q_{n-2}	Q_{n-1}	Q_n

Se opera así

$$P_k = q_kP_{k-1} + P_{k-2}$$

$$Q_k = q_kQ_{k-1} + Q_{k-2}$$

donde se ha puesto

$$P_0 = 1, \quad P_{-1} = 0$$

$$Q_0 = 0, \quad Q_{-1} = 1$$

En el ejemplo $a = \frac{943}{23} = 41$ y $b = \frac{414}{23} = 18$

$$41 = 2 \cdot 18 + 5$$

$$18 = 3 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

El esquema es entonces

		2	3	1	1	2	
0	1	2	7	9	16	<u>41</u>	= a
1	0	1	3	4	7	<u>18</u>	= b

y se sigue que $16 \cdot 18 - 7 \cdot 41 = 1$.

Continuemos con el estudio del m. c. d. en relación con la divisibilidad. En la proposición siguiente se reúnen propiedades típicas del m. c. d. .

4.5. **Proposición.** Sean a, b, c, d y k enteros. Se satisfacen las siguientes propiedades:

i) $(a, b) = d \Rightarrow (\frac{a}{d}, \frac{b}{d}) = 1 \quad (d \neq 0)$.

ii) $(a, b) = d \Rightarrow (k \cdot a, k \cdot b) = |k| \cdot d$.

iii) $(a, b + k \cdot a) = (a, b)$.

iv) $(a, b) = d$ y $(c, b) = 1 \Rightarrow (a \cdot c, b) = d$.

v) Sean $(a, b) \neq (0, 0)$. Sea $k \in N$. Entonces $k|a$ y $k|b \Rightarrow k \leq (a, b)$. O sea, (a, b) es el mayor divisor común de a y b.

Demostraciones

i) Escribamos $d = r \cdot a + s \cdot b$, donde r y s son enteros, y dividamos por a para obtener $1 = r \cdot \frac{a}{d} + s \cdot \frac{b}{d} \left((\frac{a}{d}, \frac{b}{d}) = 1 \right)$.

42 ii) Supongamos $k > 0$. Entonces $d|a$ y $d|b \Rightarrow k \cdot d | k \cdot a$ y $k \cdot d | k \cdot b$, por lo tanto $k \cdot d | (k \cdot a, k \cdot b)$. Si $d = (a, b) = r \cdot a + s \cdot b$, se tiene $k \cdot d = r \cdot k \cdot a + s \cdot k \cdot b$, de donde se sigue que $(k \cdot a, k \cdot b) | k \cdot d$. Por lo tanto, $k \cdot d = (k \cdot a, k \cdot b)$.

iii) Sean $d = (a, b)$ y $d' = (a, b + k \cdot a)$. Es claro que $d | d'$. Ahora $d' | a$ y $d' | b + k \cdot a \Rightarrow d' | a$ y $d' | b$, por lo tanto $d' | d$. O sea $d = d'$.

Se deja a cargo del lector la demostración de las propiedades restantes.

4.6. **Nota. Sugerencia Universal en Aritmética:** Si $(a, b) = d$, entonces existen u, $v \in Z$ tales que $d = u \cdot a + v \cdot b$.

$(a, b) = u \cdot a + v \cdot b$; u, $v \in Z$ se denomina una representación del m. c. d. de a y b como combinación lineal entera de a y b. Dicha representación no es única. Por ejemplo, $(6, 4) = 2$,

$$\begin{aligned} 2 &= 2 \cdot 4 + (-1) \cdot 6 \\ &= (2 + 3) \cdot 4 + (-1-2) \cdot 6 \\ &= (2 + 6) \cdot 4 + (-1-4) \cdot 6 \end{aligned}$$

En general, si $(a, b) = u \cdot a + v \cdot b$ y t es múltiplo de a y b; $t = a \cdot h = b \cdot r$.

$$\begin{aligned} &(u + h) \cdot a + (v - r) \cdot b \\ &= u \cdot a + v \cdot b + h \cdot a - r \cdot b = (a, b) \end{aligned}$$

4.7. Proposiciones

1. Sean a y b enteros. Entonces a y b son *coprimos* si, y sólo si, $(a, b) = 1$.

2. Sean a y p enteros, con p primo. Entonces a y p son coprimos si, y sólo si, $p \nmid a$. En efecto, supóngase que p es positivo (para no complicar la escritura con valores absolutos), y escribamos $d = (a, p)$. Puesto que $d | p$, debe ser $d = p$ o $d = 1$. Por lo tanto

$$d = (a,p) = 1 \Rightarrow p \nmid a$$

$$d = (a,p) \neq 1 \Rightarrow (a,p) = p \Rightarrow p | a$$

3. **Ejemplo.** Si p es primo, entonces p y $p-1$ son coprimos o, mejor, p y $(p-1)!$ son coprimos.

4. **Teorema.** Sea $p \in Z$, $p \neq \pm 1$. Entonces p es primo si, y sólo si, toda vez que divide un producto $a \cdot b$ de enteros divide necesariamente a uno de ellos. Su representación en símbolos es:

$$p \text{ primo} \Leftrightarrow \{\forall a,\ b \in Z,\ p | a \cdot b \Rightarrow p | a \text{ o } p | b\}$$

Demostración. Para no complicar la notación, ésta se limitará al caso $p > 0$. Sean p primo y $p | a \cdot b$, a y b enteros. Si $p | a$ no hay nada que probar. Sea, pues, $p \nmid a$. Entonces, por lo dicho más arriba, p y a son coprimos. Puede escribirse

$$1 = r \cdot a + s \cdot p$$

por lo tanto (multiplicando por b)

$$b = r \cdot a \cdot b + s \cdot p \cdot b$$

puesto que $p | a \cdot b$ y $p | p$ se concluye que $p | b$. Se ha probado que $p | a$ o $p | b$.

Veamos la recíproca. Sea p con esa propiedad. Razonemos por el absurdo. Supongamos, que p no es primo. Pueden encontrarse enteros positivos a y b tales que $p = a \cdot b$ con, además, $1 < a < p$, $1 < b < < p$. Es claro que $p \nmid a$ y $p \nmid b$ y que $p | a \cdot b$, pero esto contradice la propiedad inicialmente atribuida a p y el teorema queda probado.

Otro resultado importante en aritmética es el siguiente:

5. **Teorema.** Sean a, b y c enteros. Entonces

i) $(a, b) = 1$, $a | c$, y $b | c$ implican $a \cdot b | c$,

ii) $(a, c) = 1$ y $a | b \cdot c$ implican $a | b$.

Demostración

i) Escribamos

$$1 = (a, b) = r \cdot a + s \cdot b$$

por lo tanto $c = r \cdot c \cdot a + s \cdot c \cdot b$ y además se tiene

$$c = a' \cdot a = b' \cdot b, \text{ con } a', b' \in Z$$

y así resulta

$$c = r \cdot b' \cdot a \cdot b + s \cdot a' \cdot a \cdot b = (r \cdot b' + s \cdot a') \cdot a \cdot b$$

que dice que $a \cdot b | c$.

ii) Se deja como ejercicio para el lector

Las siguientes generalizaciones de los dos resultados anteriores son válidas:

j) si p es primo y $p | \Pi_{i=1}^{n} a_i$, entonces $p | a_j$ para algún j, $1 \leq j \leq n$,

jj) si $a_1, \ldots, a_n$ son divisores de c y $1 = (a_i, a_j)$ si $i \neq j$, entonces $\Pi_{i=1}^{n} a_i | c$.

6. Aplicación. Sea p primo positivo. Entonces para todo i, $1 \leq i \leq p - 1$:

$$\binom{p}{i} \text{ es divisible por } p$$

En efecto

$$\binom{p}{i} = \frac{(p \cdot (p-1) \ldots (p-(i-1))}{i!}$$

Como $\binom{p}{i} \in Z$, se sigue que $i!$ divide a $p \cdot (p - 1) \ldots (p - (i - 1))$. Puesto que $i < p$, resulta que $i!$ es coprimo con p. (Lector, justifique en detalle está afirmación.) Por lo tanto, $i!$ divide al factor $(p - 1) \ldots$ $\ldots (p - (i - 1))$, lo cual asegura que

$$\binom{p}{i} = p \cdot \frac{(p-1) \ldots (p-(i-1))}{i!}$$

es múltiplo de p.

Por ejemplo:

$$\binom{7}{1} = 7$$

$$\binom{7}{2} = \frac{7 \cdot 6}{2} = 7 \cdot 3$$

$$\binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 7 \cdot 5$$

$$\binom{7}{4} = \frac{7 \cdot 6 \cdot 5 \cdot 4}{4 \cdot 3 \cdot 2} = 7 \cdot 5$$

$$\binom{7}{5} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3}{5 \cdot 4 \cdot 3 \cdot 2} = 7 \cdot 3$$

$$\binom{7}{6} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} = 7.$$

De aquí resulta el importante resultado aritmético: "Si a y b son enteros y p es un primo, entonces $(a + b)^p = a^p + b^p + k \cdot p$", donde $k \cdot \cdot p$ indica un múltiplo entero de p. (Como se verá más adelante, esto se escribe más propiamente en la forma $(a + b)^p \equiv a^p + b^p$ módulo p o mód. (p).)

4.8. Ejercicios

1. Muestre con un contraejemplo que la afirmación anterior no es cierta si p no es primo.

2. Probar que para todo $n \in N$, $\binom{2n}{n}$ es divisible por $n + 1$.

3. Si a es primo con 240, entonces $240 | a^4 - 1$. En efecto, como $240 = 2^4 \cdot 3 \cdot 5$ será cuestión de probar que $a^4 - 1$ es divisible por 2^4, por 3 y por 5.

Escribamos $a^4 - 1 = (a^2 - 1)(a^2 + 1)$. Por la hipótesis, $a = 2k + 1$ para algún k, por lo tanto $2^3 | a^2 - 1$ y, como $2 | a^2 + 1$, se sigue que $2^4 | | a^4 - 1$. Puesto que $3 \nmid a$ puede escribirse $a = 3h + 1$ o $a = 3h + 2$. Entonces es claro que $3 | a^2 - 1$. Finalmente, dado que los restos cuadráticos no nulos módulo 5 son 1 y 4, se tiene $5 | a^2 - 1$ en el primer caso y $5 | a^2 + 1$ en el segundo. La afirmación queda completamente demostrada.

4. Hallemos todos los $a \in N$, $a > 2$, tales que verifiquen las condiciones siguientes

i) $2 | a$,

ii) $3 | a + 1$,

iii) $4 | a + 2$,

iv) $5 | a + 3$.

Por i) se tiene $a = 2x$, con $x > 1$. Por iii) x es impar, $x = 2k + 1$, o sea $a = 4k + 2$. Se sigue de ii) que $3 | k$, o sea $a = 12 \cdot h + 2$. Pero, por iv), $5 | h$, con lo que $a = 60n + 2$. El mínimo $a > 2$ con esas propiedades es 62.

5. **Ejemplo.** Hallar todos los números enteros positivos de tres cifras divisibles por 9 y por 11.

Solución. Por ser 9 y 11 coprimos, los múltiplos de 9 y 11 son exactamente los múltiplos de $9 \times 11 = 99$. Los de tres cifras son: $99 \cdot \cdot i$, $i = 2, \ldots, 10$.

4.9. Ejemplos

1. Sean a y b enteros *coprimos*. Se trata de calcular los valores posibles de $m = (3a - b,\ 2a + b)$. Supongamos $m \neq 1$. Sea p *primo* tal que $p|m$, p positivo. Entonces puede escribirse

$$3a - b = p \cdot x$$

$$2a + b = p \cdot y, \qquad x \text{ e } y \text{ en } Z$$

y se obtiene

$$5a = p \cdot (x + y)$$

$$5b = p \cdot (3y - 2x)$$

por lo tanto (véase la propiedad 4.9.4.)

$$(p|5 \text{ o } p|a) \text{ y } (p|5 \text{ o } p|b)$$

Pero esta proposición es lógicamente equivalente a la siguiente:

$$p|5 \text{ o } (p|a \text{ y } p|b)$$

Puesto que $(a, b) = 1$, se concluye que $p|5$ o sea $p = 5$.

En conclusión, si el m. c. d. no es 1, el único primo positivo que los divide es 5. Pero el análisis precedente también prueba que la máxima potencia de 5 que lo divide es 1. Por lo tanto, $(3a - b,\ 2a + b) = 1$ ó 5.

2. Sean a y b enteros *coprimos*. Se calcularán los valores posibles de

$$m = (2a - 5b,\ 4a + 3b)$$

Si $m \neq 1$, sea p *primo* tal que $p|m$. Entonces puede escribirse

$$2a - 5b = p \cdot x$$

$$4a + 3b = p \cdot y \qquad x \text{ e } y \text{ en } Z$$

Operando resulta

$$26a = p \cdot (5y + 3x)$$

$$26b = p \cdot (2y - 4x)$$

por lo tanto

$$(p|26 \text{ o } p|a) \text{ y } (p|26 \text{ o } p|b)$$

es decir

$$p|26 \text{ o } (p|a \text{ y } p|b)$$

Se concluye que

$$p \mid 2 \text{ o } p \mid 13, \text{ o sea } p = 2 \text{ o } p = 13$$

Obsérvese que $p^2 \nmid 26$, si $p = 2$ o $p = 13$. En definitiva

$$(2a - 5b,\ 4a + 3b) = 1 \ ó \ 2 \ ó \ 13 \ ó \ 26$$

3. Sean a y b enteros *coprimos*. Sean r, s, t y u enteros. Sea $d = r \cdot s - t \cdot u$. Luego para *todo primo* p probar que:

$$p \mid (ra + tb,\ ua + sb) \Rightarrow p \mid d$$

En efecto, sea

$$m = (ra + tb,\ ua + sb)$$

Entonces puede escribirse

$$ra + tb = m \cdot x$$

$$ua + sb = m \cdot y$$

Al resolver este sistema de ecuaciones, a partir del valor $d = r \cdot s - t \cdot u$, resulta

$$da = m \cdot (sx - ty)$$

$$db = m \cdot (my - ux)$$

y como $p \mid m$ se obtiene que $p \mid d$ o $p \mid a$ y $p \mid d$ o $p \mid b$. Si $(a, b) = 1$, entonces $p \mid d$ como se quiso demostrar.

En particular notemos, como corolario, que $(a, b) = 1$, $rs - tu = 1 \Rightarrow (ra + tb,\ ua + sb) = 1$.

4. Sean a, $b \in N$, coprimos. Sea $m \in Z$. Si se conoce el resto de la división de m por a y el resto de la división de m por b, hallar el resto de la división de m por $a \cdot b$.

Sean entonces

$$m = a \cdot q + r, \qquad 0 \leq r < a$$

$$m = b \cdot t + s, \qquad 0 \leq s < b$$

Sean, además, u, $v \in Z$ tales que $1 = u \cdot a + v \cdot b$. Puede escribirse

$$b \cdot m = a \cdot b \cdot q + b \cdot r$$

$$a \cdot m = a \cdot b \cdot t + a \cdot s$$

y también

$$v \cdot b \cdot m = a \cdot b \cdot v \cdot q + b \cdot r \cdot v$$

$$u \cdot a \cdot m = a \cdot b \cdot u \cdot t + a \cdot s \cdot u$$

Sumando resulta

$$m = a \cdot b \cdot q' + (b \cdot r \cdot v + a \cdot s \cdot u)$$

y el resto buscado resultará de dividir $b \cdot r \cdot v + a \cdot s \cdot u$ por $a \cdot b$. Por ejemplo, si $a = 15$, $b = 11$. Sean $r = 7$ y $s = 8$. No se necesita conocer m. Dado que $1 = 3 \cdot 15 + (-4) \cdot 11$ debe calcularse el resto de la división de $11 \cdot 7 \cdot -4 + 15 \cdot 8 \cdot 3 = 52$ por 165. El resto buscado es 52.

5. Escribir la fracción $\frac{98}{23 \cdot 89}$ en la forma: $A + \frac{B}{23} + \frac{C}{89}$, con A, B y C enteros tales que $1 \leq B < 23$, $1 \leq C < 89$.

Solución. Utilizando el A. D. se obtiene la relación $1 = 31 \cdot 23 - 8 \cdot 89$. Por lo tanto

$$\frac{1}{23 \cdot 89} = \frac{31}{89} - \frac{8}{23} = -1 + \frac{31}{89} + \frac{15}{23}$$

o sea

$$\frac{98}{23 \cdot 89} = -98 + \frac{98 \cdot 31}{89} + \frac{98 \cdot 15}{23} = -98 + 34 + \frac{12}{89} + 63 + \frac{21}{23}$$

$$= -1 + \frac{21}{23} + \frac{12}{89}$$

6. Escribir la fracción $\frac{1}{13 \cdot 18 \cdot 23}$ en la forma $A + \frac{B}{13} + \frac{C}{18} + \frac{D}{23}$ con A, B, C y D enteros tales que $1 \leq B < 13$, $1 \leq C < 18$, $1 \leq D < 23$.

Solución. Escribamos $1 = 4 \cdot 23 - 7 \cdot 13$

$$1 = 9 \cdot 18 - 7 \cdot 23$$

$$1 = 7 \cdot 13 - 5 \cdot 18$$

Se tiene $18 = 4 \cdot (23 \cdot 18) - 7 \cdot (13 \cdot 18)$

$$13 = 9 \cdot (18 \cdot 13) - 7 \cdot (23 \cdot 13)$$

y también $-5 \cdot 18 = -20 \cdot (23 \cdot 18) + 35 \cdot (13 \cdot 18)$

$$7 \cdot 13 = 63 \cdot (18 \cdot 13) - 49 \cdot (23 \cdot 13)$$

Sumando resulta $1 = 98 \cdot (18 \cdot 13) - 49 \cdot (13 \cdot 23) - 20 \cdot (23 \cdot 18)$

y finalmente $\frac{1}{13 \cdot 18 \cdot 23} = \frac{98}{23} - \frac{49}{18} - \frac{20}{13} = -1 + \frac{6}{23} + \frac{5}{18} + \frac{6}{23}$.

7. **Ejemplo.** Hallar todos los $m \in Z$ tales que $13|(15m + 14)^{18}$. Se tiene (¡dado que 13 es primo!):

$$13|(15m + 14)^{18} \Leftrightarrow 13|15m + 14 \Leftrightarrow 13|2m + 1 \Leftrightarrow$$

$$\Leftrightarrow \exists \iota \in Z \text{ tal que } 2m + 1 = 13 \cdot \iota \Leftrightarrow \exists \iota \text{ impar tal que } m = \frac{13\iota - 1}{2}.$$

Las soluciones son $\{\frac{13\iota - 1}{2} | \iota \in Z \text{ impar}\}$.

8. **Ejemplo.** Sea p un número primo > 3. Luego p^2 es de la forma $24 \cdot m + 1$, para un entero m conveniente (por ejemplo, $5^2 = 24 \cdot 1 + 1$; $7^2 = 2 \cdot 24 + 1$; $11^2 = 5 \cdot 24 + 1, \ldots$). Probemos esta afirmación.

Escribamos $p = 3 \cdot k + r$ con $r = 1$ o $r = 2$ y analicemos estos casos por separado:

$r = 1$) $p > 3$ implica que $p - 1$ es par. Además, $p - 1 = 3 \cdot k$, por lo tanto, $k = 2 \cdot h$. Entonces

$$p^2 = (3 \cdot k + 1)^2 = (3 \cdot 2 \cdot h + 1)^2 = 3 \cdot 4 \cdot h \cdot (3 \cdot h + 1) + 1$$

pero $h \cdot (3h + 1)$ es par, por lo tanto $p^2 = 24m + 1$.

$r = 2$) $p = 3k + 2$, y por ser p impar, implica que $k = 2h + 1$. Por lo tanto

$$p^2 = (3 \cdot (2h + 1) + 2)^2 = (6h + 5)^2 = 12h\,(3h + 5) + 24 + 1$$

y puesto que $h \cdot (3h + 5)$ es par, resulta $p^2 = 24m + 1$, que es lo que se quiso demostrar.

9. Sean $a,\ b,\ p \in N$, p primo impar, $(a, b) = 1$.

Probemos que $d = \left(a + b,\ \dfrac{a^p + b^p}{a + b}\right) = 1$ o p. En efecto, sean

$$a + b = dx$$

$$a^p + b^p = (a + b)dy = d^2xy$$

donde $x,\ y \in N$. Utilizando la fórmula del binomio se obtiene

$$d^2xy = (dx - b)^p + b^p = (dx)^p - p(dx)^{p-1}b + \ldots$$

$$\ldots + p(dx)b^{p-1} - b^p + b^p$$

Se sigue que $d^2x|pdxb^{p-1}$ o también $d|pb^{p-1}$. Puesto que $d|a + b$, de $(a, b) = 1$ se sigue que $(d, b) = 1$, por lo tanto $d|p$ o sea $d = 1$ o $d = p$.

10. **Problema.** Probar que no existe ningún polinomio $f(X)$ con coeficientes *enteros* tal que $f(1) = 2$ y $f(3) = 5$.

Solución. Sea $g(X) = f(X) - 2$. Se tiene que $g(X)$ es un polinomio con coeficientes enteros tal que $g(1) = 0$. Por lo tanto, $g(X) = (X - 1) \cdot h(X)$, donde $h(X)$ es un polinomio con coeficientes enteros. Si se evalúa en $X = 3$, se tiene $3 = g(3) = 2 \cdot h(3)$ *en* Z, lo que es absurdo. Por consiguiente, no existe tal $f(X)$.

11. Ejemplo. Sean $a \in N$ y $n, m \in N$. Entonces $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$. Supóngase $m < n$. Según el procedimiento de cálculo del m. c. d., a partir del Algoritmo de Euclides se tiene

$$\begin{aligned} n &= m \cdot q_1 + r_1, \quad 0 < r_1 < m \\ m &= r_1 \cdot q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2 \cdot q_3 + r_3, \quad 0 < r_3 < r_2 \\ &\dots \qquad\qquad\quad \dots \\ r_{k-2} &= r_{k-1} \cdot q_k + r_k, \quad 0 < r_k < r_{k-1} \\ r_{k-1} &= r_k \cdot q_{k+1} \end{aligned}$$

con lo que $(m, n) = r_k$. Veamos cómo estas expresiones determinan sendas expresiones en potencias de a que darán lugar al cálculo de $(a^n - 1, a^m - 1)$. En efecto, se tiene

$$a^n - 1 = (a^{m \cdot q_1} - 1) \cdot a^{r_1} + (a^{r_1} - 1), \qquad 0 < a^{r_1} - 1 < a^m - 1$$

o también, teniendo en cuenta que $a^m - 1 \mid (a^m)^q - 1$

$$a^n - 1 = (a^m - 1) \cdot t^1 + (a^{r_1} - 1), \qquad 0 < a^{r_1} - 1 < a^m - 1$$

para algún entero t_1. Por lo tanto

$$(a^n - 1, a^m - 1) = (a^m - 1, a^{r_1} - 1)$$

Iterando este proceso se llega a

$$\begin{aligned} (a^n - 1, a^m - 1) &= \dots = (a^{r_{k-1}} - 1, a^{r_k} - 1) \\ &= a^{r_k} - 1, \quad \text{pues } a^{r_k} - 1 \mid a^{r_{k-1}} - 1 \\ &= a^{(n,m)} - 1 \end{aligned}$$

12. Ejemplo. Sean $a, n, m \in N$, $n \neq m$. Entonces

$$(a^{2^n} + 1, a^{2^m} + 1) = \begin{cases} 1 & \text{si } a \text{ es par} \\ 2 & \text{si } a \text{ es impar} \end{cases}$$

Supongamos $n < m$, $m = n + k$, con $k \in N$. Si el m. c. d. no es 1, sea $p \in N$ un número que lo divide. Se tiene

$$a^{2^n} + 1 = p \cdot x, \quad a^{2^m} + 1 = p \cdot y, \text{ con } x \text{ e } y \text{ enteros.}$$

También

$$a^{2^n} = p \cdot x - 1$$

Elevando a la potencia 2^k y aplicando la fórmula del binomio, puede escribirse:

$$a^{2^m} = p \cdot z + 1 \quad \text{con } z \in Z$$

Pero, dado que $a^{2^m} = -1 + p \cdot y$, al restar resulta $p(y - z) = 2$ y $p = 1$ o $p = 2$. Por lo tanto,

$$(a^{2^n} + 1,\ a^{2^m} + 1) = 1 \text{ si } a \text{ es par}$$

$$(a^{2^n} + 1,\ a^{2^m} + 1) = 2 \text{ si } a \text{ es impar}$$

Consecuencia. Si se toma por ejemplo, $a = 2$, se tiene que la sucesión de enteros positivos $2^{2^n} + 1$ está formada por enteros coprimos dos a dos. Puesto que todo entero mayor que 1 es divisible por un primo, se concluye una vez más que hay infinitos primos en Z.

A manera de aplicación de los resultados anteriores, probemos el siguiente teorema clásico, debido a Fermat.

4.10. Teorema. Sean p un primo positivo y x e $y \in N$ tales que $p \mid x^2 + y^2$. Entonces existen $a, b \in N$ tales que $p = a^2 + b^2$.

Demostración. Escribamos $x^2 + y^2 = p \cdot m$, $m > 0$ y siempre se pueden expresar x e y como:

$$x = \dot{p} + r, \quad |r| \leq \frac{p}{2}$$

$$y = \dot{p} + s, \quad |s| \leq \frac{p}{2}$$

donde $\dot{p}$ denota un múltiplo de p. Se sigue de las relaciones anteriores que $p \mid r^2 + s^2$, $p \nmid r$, $p \nmid s$ y, además, si escribimos $r^2 + s^2 = p \cdot m_0$ es $0 < m_0 < p$.

Si $m_0 = 1$, nada queda por probar. Supongamos $m_0 > 1$. Utilizando el algoritmo de división resulta

$$x = \dot{m}_0 + x_1, \quad |x_1| \leq \frac{m_0}{2}$$

$$y = \dot{m}_0 + y_1, \quad |y_1| \leq \frac{m_0}{2}$$

Se sigue, al igual que más arriba, que $m_0 \mid x_1^2 + y_1^2$ y, si escribimos $x_1^2 + y_1^2 = m_0 \cdot m_1$, es $0 < m_1 < m_0$.

Luego

$$p \cdot m_0^2 \cdot m_1 = (r^2 + s^2) \cdot (x_1^2 + y_1^2) = (rx_1 + sy_1)^2 + (ry_1 - sx_1)^2 = X^2 + Y^2$$

con $X = rx_1 + sy_1$ e $Y = ry_1 - sx_1$. Nótese que $m_0|X$ y $m_0|Y$, o sea $X = m_0 \cdot h$, $Y = m_0 \cdot k$. Además. $p\nmid X$ y $p\nmid Y$, pues de otro modo

$$p^2|X^2 + Y^2, \quad \text{o sea } p^2|p \cdot m_0^2 \cdot m_1, \quad \text{o sea } p|m_0 \text{ o } p|m_1$$

lo que es imposible, pues $0 < m_1 < m_0 < p$.

Se concluye que

$$p \cdot m_1 = h^2 + k^2,\ p\nmid h,\ p\nmid k, 0 < m_1 < p,\ m_1 < m_0$$

Podemos aplicar descenso infinito y concluir que m_0 debe ser 1 y el teorema queda demostrado.

Nota. Una consecuencia importante de este teorema, que se verá más adelante, es el siguiente corolario: un primo p impar positivo es suma de dos cuadrados si, y sólo si, es de la forma $4k + 1$.

Nota. Este tipo de demostración suele llamarse "Método de Fermat de descenso infinito" y puede describirse así: Si una propiedad la suponemos cierta para un número positivo y deducimos que es cierta para un número positivo *menor estrictamente*, la propiedad es falsa. En efecto, por B. O. si una propiedad es cierta para un número positivo, entonces existe un número positivo *mínimo* que la satisface.

4.11. Generalización del Máximo Común Divisor. Sean $a_1, a_2, \ldots, a_n$ enteros no todos cero. Existe entonces un entero positivo d con las siguientes propiedades:

i) $d|a_i$, cualquiera que sea $i = 1, \ldots, n$,

ii) existen enteros u_i, $i = 1, \ldots, n$ tales que $d = \sum_{i=1}^{n} u_i \cdot a_i$.

En efecto, se razona inductivamente empezando por $n = 2$ (caso ya estudiado). Supongamos cierta la afirmación para $n \geq 2$ y probémosla para $n + 1$. Sean, pues, $a_1, \ldots, a_n, a_{n+1}$ enteros no todos cero. Sin (con) pérdida de generalidad, cabe suponer que $a_{n+1} \neq 0$. Entonces, si $a_1 = \ldots = a_n = 0$, $d = |a_{n+1}|$ satisface nuestros requerimientos, pues

$$|a_{n+1}|\,|a_i, \quad \text{para todo } i = 1, \ldots, n + 1$$

$$|a_{n+1}| = 1 \cdot a_1 + \ldots + 1 \cdot a_n \pm 1 \cdot a_{n+1}$$

Si no todos los $a_1, \ldots, a_n$ son cero, está definido, por la hipótesis inductiva, el m. c. d. d' de $a_1, \ldots, a_n$ y existen $u_1, \ldots, u_n$ tales que

$$d' = u_1 \cdot a_1 + \ldots + u_n \cdot a_n$$

Sean $d = (d', a_{n+1})$ y u'' y v tales que $d = u'' \cdot d' + v \cdot a_{n+1}$. Se afirma que d tiene las propiedades buscadas. Primeramente

i) $d|d'$ y $d'|a_i$ $i = 1, \ldots, n$ implican $d|a_i = 1, \ldots, n$,

ii) $d|a_{n+1}$.

Además

iii) $d = u'' \cdot d' + v \cdot a_{n+1} = u'' \cdot (u_1 \cdot a_1) + \ldots + (u_n \cdot a_n) + v \cdot a_{n+1}$.

En consecuencia, vale el paso inductivo y la afirmación queda probada.

Es fácil ver la unicidad del d de la afirmación anterior. d se denomina al m. c. d. de $a_1, \ldots, a_n$ y se denota por $d = (a_1, a_2, \ldots, a_n)$.

Adviértase que en la demostración se vio cómo obtener el m. c. d.:

$$(a_1, \ldots, a_n, a_{n+1}) = ((a_1, \ldots, a_n), a_{n+1})$$

Así, para el caso $n = 3$, se tendría $(a, b, c) = ((a, b), c)$.

4.12. Ejemplos. $(6, 15, 10) = 1$, $(2, 0, -4) = 2$, $(10, 35, 70) = 5$.

5

MINIMO COMUN MULTIPLO

Sean a y b enteros, ambos no nulos. Entonces $a \cdot b$ y $-a \cdot b$ son múltiplos de a y de b. De aquí se sigue que a y b poseen un múltiplo común > 0. O sea, el conjunto H de múltiplos comunes positivos de a y b es no vacío.

Dado que N es B. O. , puede determinarse en este conjunto H un elemento minimal que se denota por m. Las propiedades de m son las siguientes:

m1) m es múltiplo de a y de b,

m2) $m > 0$,

m3) si $k \in Z$, $k > 0$, k múltiplo de a y b, entonces $m \leq k$.

5. 1. **Definición.** m, asociado a a y b, se denomina *mínimo común múltiplo* (m. c. m.) de a y b, y se denota por $[a, b]$. Si a o b es 0, se define $[a, b] = 0$.

5. 2. **Ejemplo.** Hallemos el m. c. m. de 8 y 14. Escribamos los múltiplos de ambos números y busquemos el menor común a ambos:

8: 8, 16, 24, 32, 40, 48, <u>56</u>, ...

14: 14, 28, 42, <u>56</u>, 72, ...

Se tiene $[8, 14] = 56$.

5. 3. **Ejercicios**

1. Completar y demostrar:

i) Si $a \in Z$, entonces $[a, a] = \dots$.

ii) Si $a, b \in Z$, $[a, b] = b$ si, y sólo si, ... ?

iii) $(a, b) = [a, b]$ si, y sólo si, ... ?

iv) $[a, b] = |a \cdot b|$ si, y sólo si, ...

2. Demostrar las siguientes proposiciones:

i) $[a, b] = [b, a]$,

ii) $[[a, b], c] = [a, [b, c]]$,

iii) $a|b$, si $[a,b] = |b|$. Luego $[a,a] = |a|$,

iv) $[a, 1] = |a|$

v) $c > 0$ implica $[ac, bc] = [a, b] \cdot c$,

vi) $d > 0$, $d|a$ y $d|b$ implican $[\frac{a}{d}, \frac{b}{d}] = \frac{[a,b]}{d}$.

3. Definir el m. c. m. de cualquier número finito de enteros y calcular:

$[18, 15, 24]$, $[16, 25, 32]$, $[5, 7, 13]$, $[0, 1, -2]$, $[2, -3, 7, -7]$.

5. 4. Proposición. Sean a y b enteros no nulos. Entonces, si $k \in Z$ $a|k$ y $b|k$ implican $[a,b]|k$.

Demostración. En virtud del algoritmo de división puede escribirse

$$k = [a, b] \cdot q + r \quad 0 \leq r < [a, b]$$

Puesto que de $a|k$ y $a|[a,b]$ se sigue que $a|r$, análogamente $b|r$, o sea r es múltiplo común de a y b. De la misma definición de $[a,b]$ (... multiplo común minimal...) se sigue que $r = 0$ con lo que $[a,b]|k$ como se quiso demostrar.

Demostremos una propiedad importante que liga a (a, b) con $[a, b]$ y que además proporciona una forma de calcular $[a,b]$, conocido (a, b) y viceversa.

5. 5. Teorema. Sean a y b enteros no nulos, entonces

$$|a \cdot b| = (a, b) \cdot [a, b]$$

Demostración. Se demostrará que $m = \frac{|a \cdot b|}{(a, b)}$ es el m. c. m. de a, b.

i) $[a,b]$ divide a m. En efecto, si se escribe

$$m = \frac{|a \cdot b|}{(a, b)} = \frac{|a|}{(a, b)} \cdot |b| = |a| \cdot \frac{|b|}{(a, b)}$$

resulta que m es múltiplo de a y de b, por lo que la proposición anterior asegura que $[a,b]|m$, como se quería probar.

ii) m divide a $[a,b]$. En efecto, escribamos

$$(a, b) = r \cdot a + s \cdot b, \text{ o sea } 1 = r \cdot \frac{a}{(a, b)} + s \cdot \frac{b}{(a, b)}$$

y también $[a, b] = r \cdot \frac{a}{(a, b)} \cdot [a, b] + s \cdot \frac{b}{(a, b)} \cdot [a, b]$.

Si se escribe $[a, b] = b' \cdot b = a' \cdot a$, $a' \in Z$, $b' \in Z$, resulta finalmente

$$[a, b] = r \cdot b' \cdot \frac{a \cdot b}{(a, b)} + s \cdot a' \cdot \frac{a \cdot b}{(a, b)} =$$

$$= \frac{a \cdot b}{(a,b)} (r \cdot b' + s \cdot a')$$

lo cual demuestra que m divide a $[a, b]$. De i) e ii) resulta la tesis.

5.6. **Corolario.** Sean a y b enteros no nulos coprimos, entonces $[a, b] = |a \cdot b|$.

Demostración. En efecto, al ser coprimos, es $(a, b) = 1$.

5.7. **Problema.** Sean a y b enteros positivos. Dados (a, b) y $[a, b]$, encontrar a y b.

Solución. Se tiene $a = (a, b) \cdot x$, $b = (a, b) \cdot y$, con $(x, y) = 1$. Además, $(a, b)\,[a, b] = a \cdot b = (a, b)^2 \cdot x \cdot y$, es decir $\frac{[a,b]}{(a,b)} = x \cdot y$. Luego las soluciones posible son:

$$a = (a, b) \cdot x, \quad b = (a, b) \cdot y, \text{ con } (x, y) = 1, \text{ y } x \cdot y = \frac{[a,b]}{(a,b)}$$

Por ejemplo, dados $(a, b) = 36$, $[a, b] = 756$, se tiene $\frac{[a,b]}{(a,b)} = 21 = 3 \cdot 7 = 1 \cdot 21$. Las soluciones son pues

$$a = 108, \quad b = 252$$

$$a = 36, \quad b = 756$$

5.8. **Problema.** Dados $a + b$ y $[a, b]$, hallar (a, b).

Solución. Vamos a probar que $(a, b) = (a + b, [a, b])$. Sea $d = (a, b)$ y sean $a = d \cdot x$ y $b = d \cdot y$, con $(x, y) = 1$. Por lo tanto, $d^2 \cdot x \cdot y = a \cdot b = [a, b] \cdot d \Rightarrow d \cdot x \cdot y = [a, b]$. Se sigue que $(a + b, [a, b]) = (d \cdot (x + y), d \cdot x \cdot y) = d \cdot (x + y, x \cdot y) = d$, pues $(x + y, x \cdot y) = 1$.

5.9. **Problema.** Dados a y b en N, determinar cuántos múltiplos de b hay en el conjunto $\{t \cdot a \mid 1 \le t \le b\}$.

Solución. Hay un total de (a, b). En efecto, si $b \mid ta$, como $a \mid ta$, resulta $[a, b] \mid ta$, o sea

$$ta = [a, b]\, x = \frac{a \cdot b}{(a,b)}\, x \text{ o sea } t = \frac{b}{(a,b)}\, x$$

como $1 \le t \le b$, resulta $1 \le x \le (a, b)$. Recíprocamente, si $1 \le x \le (a, b)$, entonces ta es múltiplo de b, si $t = \frac{b}{(a,b)}\, x$. En consecuencia, todo enentero entre 1 y (a, b) da lugar exactamente a un múltiplo de b.

6

TEOREMA FUNDAMENTAL DE LA ARITMETICA

La propiedad más importante de los números primos es la facultad de expresar todo número entero (distinto de 0, 1 y - 1) como producto de un número finito de los mismos. A la vez, dicha forma de representación es esencialmente única (como se precisará a continuación). Por lo tanto, mucha información de Z está en los primos y de ahí que el estudio de sus propiedades sea tan importante.

6.1. Teorema Fundamental de la Aritmética (T. F. A.). Sea $n \in Z$, $n \neq 0; -1; 1$. Entonces existe una sucesión finita de primos p_i, $i = 1, \ldots, k$ tal que $0 < p_1 \leq \ldots \leq p_k$ y

$$n = \epsilon \cdot \prod_{i=1}^{k} p_i = \epsilon \cdot p_1 \ldots p_k$$

donde ϵ es 1 ó - 1.

La forma anterior de expresar n es única, o sea si q_j, $j = 1, \ldots, t$, son primos, tales que $0 < q_1 \leq \ldots \leq q_t$

$$n = \delta \prod_{j=1}^{t} q_j, \text{ con } \delta = 1 \text{ ó } -1$$

entonces

$$k = t$$

$$p_i = q_i \qquad i = 1, \ldots k = t$$

$$\epsilon = \delta$$

(Por ejemplo, $12 = 2 \cdot 2 \cdot 3$; $15 = 3 \cdot 5$; $-20 = -1 \cdot 2 \cdot 2 \cdot 5$.)

Demostración. Adviértase que el teorema es cierto, si n es ya un primo. Además, sin pérdida de generalidad, cabe suponer que n es positivo.

Supóngase que el teorema no sea cierto. Existe entonces un número entero positivo $\neq 1$, que no admite representación en producto de primos, como establece el teorema. Por B. O. existe un entero positivo minimal con esa propiedad. Sea m. Entonces m es el menor entero positivo no factorizable en producto de primos.

Es claro que m no puede ser primo, pues m satisfaría el teorema. Por lo tanto, m es divisible por algún primo positivo y sea p el menor primo que divide a m (B. O.).

Sea $m = p \cdot m'$. Puesto que $m' < m$ y $m' \neq 1$, se sigue que el teorema se cumple para m'. O sea, existen primos $p_2, \ldots, p_k$, $p_2 \leq \ldots \leq p_k$, tales que $m' = p_2 \ldots p_k$. Entonces por el carácter minimal de p, $p \leq p_2$. Resulta

$$m = p \cdot m' = p \cdot p_2 \ldots p_k$$

$$p \leq p_2 \leq \ldots \leq p_k$$

Obsérvese que ha surgido una contradicción, pues m no era factorizable. Se sigue que la primera parte del teorema, relativa a la factorización en producto de primos es verdadera.

A continuación se verá la cuestión de unicidad. A tal efecto, supongamos

$$p_1, \ldots, p_k \quad \text{primos}, \ 0 < p_1 \leq \ldots \leq p_k$$

$$q_1, \ldots, q_t \quad \text{primos}, \ 0 < q_1 \leq \ldots \leq q_t$$

tales que

$$n = p_1 \ldots p_k = q_1 \ldots q_t$$

Si $k = 1$, debe ser $t = 1$ (por definición de número primo) y en este caso vale la unicidad buscada. Supongamos que el teorema es válido para k, vamos a probarlo para $k + 1$ (o sea inducción en el número de factores primos de una descomposición). Sea pues

$$p_1 \ldots p_k \cdot p_{k+1} = q_1, \ldots, q_t$$

con p_i y q_j primos y tal que $p_i \leq p_j$ si $i \leq j$, etc.

Si se escribe $p_1 (p_2 \ldots p_{k+1}) = q_1 \ldots q_t$ resulta que $p_1 | q_1 \ldots q_t$ y, por ser p_1 primo, p_1 divide a algún q_j, $j = 1, \ldots, t$, pero, por ser p_1 y q_j primos positivos se sigue que $p_1 = q_j$.

Se escribe

$$p_2 \ldots p_{k+1} = q_1 \ldots \hat{q_j} \ldots q_t$$

donde $\hat{q_j}$ indica que debe excluirse el término de índice j.

Vamos a probar que $j = 1$. En efecto, razonando análogamente con q_1, se tiene que

$$q_1 | p_h, \text{ para algún } h = 1, \ldots, k + 1$$

Entonces $p_1 \leq p_h = q_1 \leq q_j = p_1$ con lo que $p_1 = q_1$, como se quería probar.

Por consiguiente, luego de cancelar $p_1 = q_1$, en ambos miembros resulta

$$p_2 \ldots p_{k+1} = q_2 \ldots q_t$$

El miembro izquierdo consta de k factores primos; es posible utilizar la hipótesis inductiva y concluir que $k = t - 1$, con lo que $k + 1 = t$

y

$$p_2 = q_2$$

$$\vdots$$

$$p_{k+1} = q_t$$

Como también $p_1 = q_1$, vale el paso inductivo en la demostración de la unicidad y se ha demostrado la unicidad de la factorización en producto de primos.

6.2. Nota. En virtud del Teorema Fundamental de la Aritmética se dice que Z es un *dominio de factorización única* (D. F. U.). Asimismo, por existir en Z un algoritmo de división, se dice que Z es un *dominio euclidiano* (D. E.). La propiedad de ser D. F. U. es consecuencia de la propiedad de ser D. E. Ambos tipos de propiedades se consideran situaciones más generales en lo que se llama álgebra conmutativa.

6.3. Ejemplo. No existen enteros m y n tales que $m^2 = 15 \cdot n^2$. Este hecho es consecuencia inmediata del T. F. A. Es claro que, sin perder generalidad, podemos restringirnos a m y n positivos. Entonces:

i) $m \neq 1$, pues de otro modo sería $1 = 15 \cdot n^2$, lo que es absurdo.

ii) Si $n = 1$, entonces $m^2 = 15$. Sea $m = p_1 \ldots p_k$ la factorización de m en producto de primos. Entonces

$$m^2 = (p_1 \ldots p_k) \cdot (p_1 \ldots p_k) = (p_1 \cdot p_1) \ldots (p_k \cdot p_k)$$

Además la factorización de 15 en productos de primos es $15 = 3 \cdot 5$. De $(p_1 \cdot p_1) \ldots (p_k \cdot p_k) = 3 \cdot 5$ sigue una contradicción al T. F. A. En efecto, en el miembro izquierdo, cada factor primo aparece un número par de veces, en tanto que en el derecho el factor primo 3 sólo aparece un número impar de veces. Eso contradice la unicidad establecida en el T. F. A.

Podemos, pues, suponer $n \neq 1$ y $m \neq 1$. Sean

$$m = p_1 \ldots p_k$$

$$n = q_1 \ldots q_h$$

las factorizaciones de m y n, respectivamente, en producto de primos. Entonces

$$(p_1 \cdot p_1) \ldots (p_k \cdot p_k) = m^2 = 15 \cdot n^2 =$$

$$= 3 \cdot 5 \cdot (q_1 \cdot q_1) \ldots (q_h \cdot q_h)$$

pero esta igualdad contradice al T. F. A. pues, en el miembro izquierdo, cada factor primo aparece un número par de veces, en tanto que

en el derecho el factor primo 3 aparece un número impar de veces. Esto demuestra la imposibilidad de tener enteros m y n tales que $m^2 = 15 \cdot n^2$.

Volvamos al T. F. A. Si m es un entero no nulo ni unidad y $p_1, \dots, p_s$ son los primos distintos entre sí que aparecen en su factorización, puede escribirse

$$m = p_1^{t_1} \dots p_s^{t_s}$$

con $p_1 < \dots < p_s$. Esto proviene de agrupar los factores primos iguales. Así

$$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$$

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$$

Si $n \in N$, $n \neq 1$, es claro del T. F. A. que n divide a m si, y sólo si, n admite, por factorización en producto de primos, una expresión del tipo

$$n = p_1^{i_1} \dots p_s^{i_s}, \quad \text{con } 0 \le i_1 \le t_1, \dots, 0 \le i_s \ t_s$$

6.4. Ejemplo. Se sigue de lo anterior que, dado

$$m = p_1^{i_1} \dots p_s^{i_s}, \text{ con } p_i \text{ primos; } p_i \neq p_j, \text{ si } i \neq j$$

entonces los divisores posibles de m son

$$p_1^{h_1} \dots p_s^{h_s}$$

donde los h_j pueden tomar todos los valores $0 \le h_j \le t_j$, de manera que m posee exactamente

$$(t_1 + 1) \cdot (t_2 + 1) \dots (t_s + 1) \text{ divisores positivos}$$

Así: 2^5 posee seis divisores positivos: $1, 2, 2^2, 2^3, 2^4, 2^5$.

$2^5 \cdot 3^2 \cdot 7$ posee 36 divisores positivos: $1, 2, 2^2, \dots, 3, 3^2, 5, \dots, 2^5 \cdot 3^2 \cdot 7$.

6.5. Ejemplos

1. ¿Cuál es el menor número positivo que admite exactamente 15 divisores positivos?

Solución. $15 = 3 \cdot 5$. Por lo tanto, el número tiene la forma $p^2 \cdot q^4$, con p y q primos y $p \neq q$, o también p^{14}, p primo. Se trata de hallar el menor número positivo y para ello pueden utilizarse los primos más chicos. Los casos posibles son:

$$2^{14}$$
$$2^2 \cdot 3^4$$
$$3^2 \cdot 2^4$$

2^{14} lo descartamos, pues es mayor que los otros.

Como $2^2 \cdot 3^4 = 324$ y $3^2 \cdot 2^4 = 144$; entonces, 144 es el número buscado.

2. Sean a, b y d en Z. Entonces si $a \neq 0$

$$a^2 = d \cdot b^2 \Rightarrow d \text{ es un cuadrado en } Z.$$

Si $a = 1$ ó -1, entonces $1 = d \cdot b^2$ y se sigue de inmediato que $d = 1$, cuadrado en Z.

Sea $a \notin \{1, -1\}$. Sea p un primo que aparece en la factorización de a, digamos a_p veces. Entonces p aparece $2 \cdot a_p$ veces en a^2. Veamos el miembro derecho. Sea b_p y d_p los números de ocurrencias de p en la factorización de b y d, respectivamente. El T. F. A. implica la igualdad:

$$2 \cdot a_p = d_p + 2 \cdot b_p \Rightarrow d_p \text{ par}$$

Como todo factor primo p_i de d lo es de a, resulta

$$d = p_1^{2k_1} \dots p_s^{2k_s} = (p_1^{k_1} \dots p_s^{k_s})^2$$

un cuadrado, como se quería demostrar.

Consecuencias

i) Las ecuaciones $a^2 = 2 \cdot b^2$, $a^2 = 12 \cdot b^2$, $a = 15 \cdot b^2, \dots$ no admiten solución en Z.

ii) $\frac{a^2}{b^2} \in Z$, con a y b enteros, implica $\frac{a}{b} \in Z$. En efecto:

$$\frac{a^2}{b^2} \in Z \Rightarrow b^2 | a^2 \Rightarrow a^2 = d \cdot b^2 \Rightarrow d = c^2 \Rightarrow$$

$$\Rightarrow a^2 = (c \cdot b)^2 \Rightarrow a = (\pm c) \cdot b \Rightarrow$$

$$\Rightarrow b | a \Rightarrow \frac{a}{b} \in Z$$

3. Suma de los divisores positivos de un número. Sea

$$a = \pm \prod_{i=1}^{s} p_i^{a_i} = \pm p_1^{a_1} \dots p_s^{a_s}$$

donde los p_i son primos positivos distintos entre sí y los a_i son enteros positivos. Se quiere calcular la suma de todos los divisores positivos de a.

Los divisores positivos de a coinciden con los sumandos del producto

$$(1 + p_1 + p_1^2 + \dots + p_1^{a_1}) \dots (1 + p_s + \dots + p_s^{a_s}) \text{ y}$$

la suma buscada coincide con el número precedente que puede calcularse a partir de la fórmula de la progresión geométrica para cada uno de los factores. Resulta

$$S = \frac{(p_1^{a_1+1} - 1) \ldots (p_s^{a_s+1} - 1)}{(p_1 - 1) \ldots (p_s - 1)}$$

Se deja a cargo del lector calcular el *producto* de todos los divisores positivos de a.

6.6. **Resolución de la ecuación** $x^2 + y^2 = z^2$. Si x, y y z es solución, también lo es kx, ky, kz en $k \in Z$; interesa, entonces, obtener soluciones positivas y además primitivas en el sentido que x, y y z no poseen ningún factor primo común, para lo cual es suficiente obtener las soluciones con $(x, y) = 1$.

Un ejercicio sencillo dice que de existir soluciones x, y y z en N, x e y no pueden ser ambos impares. Supongamos, entonces, que $x = 2t$ e y y z son impares. Se tiene

$$4t^2 = z^2 - y^2 = (z - y) \cdot (z + y)$$

Ambos, $z - y$ y $z + y$, son pares y, además, 4 no puede dividirlos, ya que se seguiría que z e y son pares. Puede concluirse, entonces, que

$$t^2 = \frac{z-y}{2} \frac{z+y}{2}, \text{ con } (\frac{z-y}{2}, \frac{z+y}{2}) = 1$$

Se sigue del T. F. A. que

$$\frac{z-y}{2} = u^2, \frac{z+y}{2} = v^2, \; u \text{ y } v \text{ en } N$$

Por lo tanto

$$x = 2uv, \; y = v^2 - u^2, \; z = u^2 + v^2$$

con $(u, v) = 1$ y u y v de distinta paridad.

Es claro que, dados u y v con esas propiedades, los valores de x, y y z satisfacen la ecuación $x^2 + y^2 = z^2$. Se han obtenido todas las soluciones primitivas. Como aplicación de este resultado, se probará la imposibilidad de resolver la ecuación fermatiana

$$x^4 + y^4 = z^4$$

Para ello basta probar que la ecuación $x^4 + y^4 = z^2$ no admite solución en N. Supongamos, entonces, que esa ecuación tiene solución y procedamos a elegir una que tenga el valor de z *mínimo*. Se probará que hay una solución con z positivo inferior (¡método del descenso!)

De $x^4 + y^4 = z^2$, $(x, y) = 1$, se sigue la existencia de u, $v \in N$ de distinta paridad y tales que $(u, v) = 1$ y $x^2 = 2uv$, $y^2 = v^2 - u^2$ y $z = u^2 +$

$+ v^2$. Analizando restos, no es difícil inferir que u es impar y, por lo tanto, v es par.

Dado que $x^2 = 2uv$, se tiene $(\frac{x}{2})^2 = u \cdot \frac{v}{2}$, de donde se sigue que $\frac{v}{2} = t^2$ y $u = h^2$. Consideremos la ecuación $v^2 + y^2 = u^2$. Aplicando el resultado inicial puede escribirse $v = 2sr$, $y = s^2 - r^2$, $u = s^2 + r^2$ con $(s, r) = 1$. Dado que $\frac{v}{2}$ es un cuadrado, se sigue que $s = a^2$ y $r = b^2$. En definitiva, se tiene $h^2 = u = s^2 + r^2 = a^4 + b^4$, pero ahora $h < z$, de manera que se tiene una contradicción. La ecuación $x^4 + y^4 = z^2$ no es resoluble y como consecuencia tampoco lo es $x^4 + y^4 = z^4$.

6.7. **Ejercicios**

1. ¿Existen números racionales no nulos a, b y r tales que $3(a^2 + b^2) = 7 \cdot r^2$?

2. Probar que si $n > 1$, entonces $1 + \frac{1}{2} + \ldots + \frac{1}{n}$ no es entero.

3. Probar que para todo $n \in Z$.

   i) $\frac{1}{5} n^5 + \frac{1}{3} n^3 + \frac{7}{15} n$ es entero.

   ii) $\frac{1}{7} n^7 + \frac{1}{3} n^3 + \frac{11}{21} n$ es entero.

4. Probar la no existencia de enteros m y n tales que

   i) $m^2 = 2n^2$

   ii) $m^3 = 4n^3$

   iii) $m^2 = 12n^2$

   iv) $m^4 = 27$

   v) $m^2 = 180$

   vi) $m^3 = 2n^3$

5. Probar que si $n \geq 2$, entonces $\sqrt[n]{n}$, es irracional (**Sugerencia.** Recordar que $n \geq 2 \Rightarrow 2^n > n$).

6. Representar los siguientes enteros como producto de primos:

   i) 147200

   ii) $(210)^4$

   iii) $18 \cdot 365$

   iv) $(1980)^2$

   v) $(63)^2 \cdot 18 \cdot (21)^5$

   vi) $(10!)^2 (5!)^2$

   vii) $(5!)^{5!}$

7. Hallar el menor múltiplo positivo de 945 que sea un cuadrado.

8. Hallar el número de divisores positivos de 2160 y calcular la suma.

$+ v^2$. Analizando restos, no es difícil inferir que u es impar y, por lo tanto, v es par.

Dado que $x^2 = 2uv$, se tiene $(\frac{x}{2})^2 = u \cdot \frac{v}{2}$, de donde se sigue que $\frac{v}{2} =$ $= t^2$ y $u = h^2$. Consideremos la ecuación $v^2 + y^2 = u^2$. Aplicando el resultado inicial puede escribirse $v = 2sr$, $y = s^2 - r^2$, $u = s^2 + r^2$ con $(s, r) = 1$. Dado que $\frac{v}{2}$ es un cuadrado, se sigue que $s = a^2$ y $r = b^2$. En definitiva, se tiene $h^2 = u = s^2 + r^2 = a^4 + b^4$, pero ahora $h < z$, de manera que se tiene una contradicción. La ecuación $x^4 + y^4 = z^2$ no es resoluble y como consecuencia tampoco lo es $x^4 + y^4 = z^4$.

6.7. Ejercicios

1. ¿Existen números racionales no nulos a, b y r tales que $3(a^2 + b^2) = 7 \cdot r^2$?

2. Probar que si $n > 1$, entonces $1 + \frac{1}{2} + \ldots + \frac{1}{n}$ no es entero.

3. Probar que para todo $n \in Z$.

   i) $\frac{1}{5} n^5 + \frac{1}{3} n^3 + \frac{7}{15} n$ es entero.

   ii) $\frac{1}{7} n^7 + \frac{1}{3} n^3 + \frac{11}{21} n$ es entero.

4. Probar la no existencia de enteros m y n tales que

i) $m^2 = 2n^2$	iv) $m^4 = 27$
ii) $m^3 = 4n^3$	v) $m^2 = 180$
iii) $m^2 = 12n^2$	vi) $m^3 = 2n^3$

5. Probar que si $n \geq 2$, entonces $\sqrt[n]{n}$, es irracional (**Sugerencia.** Recordar que $n \geq 2 \Rightarrow 2^n > n$).

6. Representar los siguientes enteros como producto de primos:

i) 147200	v) $(63)^2 \cdot 18 \cdot (21)^5$
ii) $(210)^4$	vi) $(10!)^2 (5!)^2$
iii) $18 \cdot 365$	vii) $(5!)^{5!}$
iv) $(1980)^2$	

7. Hallar el menor múltiplo positivo de 945 que sea un cuadrado.

8. Hallar el número de divisores positivos de 2160 y calcular la suma.

9. Para los siguientes valores de a determinar la mayor potencia de a que divide a 100! a = 3, 5, 15, 20, 25, 29, 33, 50, 75, 97, 100.

10. ¿Cuál es el menor entero positivo a tal que $\frac{9360}{a}$ es un cuadrado en N?

11. ¿Cuál es el menor número positivo que sumado a 935 da un cuadrado?

12. Hallar la mayor potencia de 7 que divide al producto $10! \cdot 20! \cdot 30! \ldots 100!$

13. ¿Cuál es el número máximo de factores primos que posee un número ≤ 100? Y ¿≤ 1000?

14. Sean a y b enteros positivos coprimos. Probar que

i) $c \in N$, $c | a \cdot b \Rightarrow$ existen d_1 y d_2 tales que $c = d_1 \cdot d_2$, $d_1 | a$, $d_2 | b$ y $(d_1, d_2) = 1$.

ii) Para todo n, a^n y b^n son coprimos.

iii) Si $a \cdot b = c^n$, entonces existen enteros positivos e y f tales que $a = e^n$ y $b = f^n$.

15. Probar que $\log_{10} 2$ es irracional. ¿Para qué valores de a es $\log_{10} a$ racional?

16. Hallar la suma y el producto de todos los divisores positivos de:

i) $2^{10} \cdot 3$,

ii) 210^{12},

iii) 10!

iv) $4^5 \cdot 9^6 \cdot 14^3$.

17. Probar que un número entero positivo es un cuadrado si, y sólo si, el número total de divisores positivos es un número impar.

18. ¿Qué polígono regular tiene:

i) 9 diagonales,

ii) 65 diagonales,

iii) 119 diagonales?

19. Hallar los menores números positivos que poseen:

i) 9 divisores,

ii) 18 divisores,

iii) 24 divisores.

20. Descomponer en producto de primos y hallar todos los divisores de:

i) 13104,

ii) 46800,

iii) 91494.

21. Calcular n sabiendo que $n \cdot (n + 1) = 992$.

22. Calcular n sabiendo que $n \cdot (n + 1) \cdot (2n + 1) = 75174$.

23. Cinco hombres recogieron en una isla un cierto número n de cocos y resolvieron repartirlos al día siguiente. Durante la noche uno de ellos decidió separar su parte y para ello dividió el total en cinco partes y dio un coco que sobraba a un mono y se fue a dormir. Enseguida, otro de los hombres hizo lo mismo, dividiendo lo que había quedado por cinco, dando un coco que sobraba a un mono y retirando su parte se fue a dormir. Uno tras otro los tres restantes hicieron lo mismo, dándole a un mono el coco que sobraba. A la mañana siguiente repartieron los cocos restantes dándole a un mono el coco sobrante.

Pregunta: ¿Cuál es el número mínimo de cocos que se recogieron?

(Solución: Se tiene las siguientes ecuaciones:

$$\begin{aligned} n &= 5k + 1 \\ 4k &= 5l + 1 \\ 4l &= 5t + 1 \\ 4t &= 5r + 1 \\ 4r &= 5h + 1 \\ 4h &= 5s + 1 \end{aligned} \quad \text{o, equivalente,} \quad \begin{aligned} n + 4 &= 5(k + 1) \\ 4(k + 1) &= 5(l + 1) \\ 4(l + 1) &= 5(t + 1) \\ 4(t + 1) &= 5(r + 1) \\ 4(r + 1) &= 5(h + 1) \\ 4(h + 1) &= 5(s + 1) \end{aligned}$$

por lo tanto $4^5 \cdot (n + 4) = 5^6 \cdot (s + 1)$. Como $(4, 5) = 1$, se sigue que $5^6 | n + 4$, o sea $n = 5^6 \cdot m - 4$. Para $m = 1$, se logra el mínimo, o sea ¡$\underline{n = 15621}$, nada menos!)

24. Hallar el número total de enteros positivos < 1000, coprimos con 120. (Respuesta: 266.)

7

NUMEROS PERFECTOS

Sean $a \in N$ y $S(a)$ la suma de la totalidad de divisores positivos de a. Se dice que a es *perfecto*, si a coincide con la suma de la totalidad de sus divisores positivos excluido el mismo a, o sea también $S(a) = 2a$.

Por ejemplo:

$$6 = 1 + 2 + 3$$
$$28 = 1 + 2 + 4 + 7 + 14$$
$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$$

i) Notar que si a es un entero positivo,

i1) a es primo si, y sólo si, $S(a) = a + 1$;

i2) si p es primo y $n \in N$, entonces $S(p^n) = 1 + p + p^2 + \dots + p^n = \frac{p^{n+1} - 1}{p - 1}$;

i3) si a y b son enteros positivos, $(a, b) = 1 \Rightarrow S(a \cdot b) = S(a) \cdot S(b)$, o sea S es una función multiplicativa.

ii) Sea p primo de la forma $p = 2^n - 1$ (por ejemplo, $3 = 2^2 - 1, 7 = 2^3 - 1$).

El número

$$2^{n-1} \cdot (2^n - 1) = p \cdot \frac{p+1}{2}$$

es perfecto. Demostrarlo como ejercicio.

iii) (Euler). Sea a un número *par* perfecto. Probar que existe un primo p de la forma $2^n - 1$ tal que

$$a = 2^{n-1} \circ (2^n - 1)$$

(**Solución.** Sea $a = 2^{n-1} \cdot b$, b impar, $n > 1$, $b > 0$

$$2a = 2^n \cdot b = S(a) = S(2^n) \cdot S(b) = \frac{2^n - 1}{2 - 1} S(b) = (2^n - 1) S(b) \therefore$$

$$\therefore S(b) = \frac{2a}{2^n - 1} = b + \frac{b}{2^n - 1}, \text{ con } \frac{b}{2^n - 1} = S(b) - b \in Z.$$

Puesto que $S(b)$ es suma de todos los divisores positivos de b, y $\frac{b}{2^n - 1} \mid b$, se sigue que $\frac{b}{2^n - 1} = 1$ y así $b = 2^n - 1$ es primo, como se quería probar.)

iv) Probar que si $a > 0$ y $n \geq 2$, entonces $p = a^n - 1$ es primo sólo si $a = 2$ y n es primo.

Notas: 1. Se sigue que los únicos números naturales perfectos *pares* son de la forma $2^{n-1} \cdot p$, con p primo de la forma $2^n - 1$.

2. Los primos de la forma $2^n - 1$ se denominan primos de Mersenne (Marin Mersenne, 1588-1648). Los únicos primos de Mersenne conocidos ocurren para $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11.213, 19.937, 21.701, 23.209, 44.497, 86.243$.

El número $2^{86243} - 1$ tiene 25962 dígitos. En efecto, si n es el número de dígitos de 2^{86243} se verifica

$$10^n > 2^{86243} > 2^{86243} - 1 > 10^{n-1}$$

por lo tanto, tomando $\log_{10}$ resulta $n > 25961 \geq n - 1$, o sea $n = 25962$. Se recomienda al lector el artículo "The Search for Prime Numbers" por Carl Pomerance publicado en *Scientific American*, diciembre de 1982. Véase también *Scientific American*, marzo 1983, pág. 11 (Letters).

3. Sobre el tema quedan aún dos problemas abiertos:

a) ¿Existen números perfectos impares?

b) ¿Existen infinitos primos de Mersenne?

8

ORDEN p-ADICO

Sean $m \in \mathbb{Z}$ y p primo. Por $\nu_p(m)$ se denota la máxima potencia de p que divide a m. Entonces, si $m \neq 0$,

$$0 \leq \nu_p(m)$$

$$p^h | m \text{ implica } h \leq \nu_p(m)$$

$$p^{\nu_p(m)} | m$$

Es claro que $p|m$ si, y sólo si,

$$\nu_p(m) > 0$$

$\nu_p(m)$ se denomina el *orden* de m respecto de p (orden p-ádico).

Definimos también $\nu_p(0) = \infty$.

Con la noción de orden se puede enunciar la condición de divisibilidad

$$m|n \text{ si, y sólo si, } (\forall\, p),\ p \text{ primo},\ \nu_p(m) \leq \nu_p(n).$$

Es de notar que si $m \neq 0$, entonces

$$\nu_p(m) = 0, \text{ para casi todo primo } p$$

(por esto debe entenderse que $\nu_p(m) = 0$ para todo p, salvo un conjunto finito de primos). Entonces el producto

$$(*) \quad \prod_p p^{\nu_p(m)}$$

donde p recorre todos los primos positivos, sólo contiene un número finito de factores $\neq 1$. Por lo tanto, aunque parezca un producto de infinitos factores, (*) tiene sentido. Pero es claro que

$$\prod_p p^{\nu_p(m)} = m$$

y es ésta la forma que adquiere el T. F. A.

Por ejemplo

$$6 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 \ldots = 2 \cdot 3$$

$$15 = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^0 \ldots = 3 \cdot 5$$

Probar la validez de

i) $|x|_p = 0 \Leftrightarrow x = 0$,

ii) $|x \cdot y|_p = |x|_p \cdot |y|_p$,

iii) $|x + y|_p \leq \text{máx}\{|x|_p, |y|_p\}$,

iv) $|x + y|_p = \text{máx}\{|x|_p, |y|_p\}$, si $|x|_p \neq |y|_p$.

7. Sea p primo > 0. Extendemos la función orden p-ádico a Q. Sea $0 \neq q \in Q$. Existen únicos r, s y t enteros tales que $q = p^r \cdot \frac{s}{t}$, tales que $p \nmid s \cdot t$, $(s, t) = 1$. Definimos $\nu_p(q) = r$. Se tiene $\nu_p: Q - \{0\} \to Z$. Probar la validez de las propiedades enunciadas en 5.

8. Extender el ejercicio 6 a la norma p-ádica sobre Q por $|0|_p = 0$ y $|x|_p = p^{-\nu_p(x)}$, si $0 \neq x = p^{\nu_p(x)} \cdot \frac{s}{t}$, con $(s, t) = 1$, y $p \nmid s \cdot t$.

a) Evaluar

i) $\nu_7(\frac{700}{197})$,

ii) $\nu_5(-0,0635)$,

iii) $\nu_2(\frac{128}{7})$,

iv) $\nu_3(\frac{7}{9})$,

v) $\nu_{13}(-\frac{26}{169})$.

La norma p-ádica permite definir sobre Q la métrica o distancia p-ádica.

b) Evaluar $|x-y|_p$ en los siguientes casos:

i) $|1-26|_5$,

ii) $|1-26|_3$,

iii) $|\frac{1}{9} + \frac{1}{16}|_5$,

iv) $|1-183|_7$.

c) ¿Qué significa decir que un número racional x satisface $|x|_p < 1$?

d) Probar que si $x \in Q$, satisface $|x|_p < 1$, $\forall_p$, entonces $x \in Z$.

Nota: La métrica p-ádica al definir una distancia sobre Q permite desarrollar un análisis "p-ádico" Se pueden definir, por ejemplo, las nociones de sucesión convergente y sucesión de Cauchy. Usando $|\ |_p$

se puede repetir la clásica construcción de R a partir de Q (vía el valor absoluto ordinario) para obtener para cada primo p un cuerpo Q_p, llamado el *cuerpo p-ádico*. Es posible demostrar que los elementos de Q_p se representan por "series" $\sum_{i=m}^{\infty} a_i p^i$, donde a_i son enteros tales que $0 \leq a_i < p$ y m es cualquier entero. Por ejemplo

$$-3 = 0 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + \ldots$$

$$-5 = 1 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + \ldots$$

$$\frac{1}{2} = 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + \ldots$$

$$\frac{1}{6} = 2 \cdot \frac{1}{3} + 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 \ldots .$$

La invención de los números p-ádicos, a fines del siglo pasado, se debe a Kurt Hensel (1861-1941), matemático alemán. En la teoría algebraica de números se han obtenido importantes resultados gracias a los números (y métodos) p-ádicos.

9

DESARROLLOS *s*-ADICOS

Comencemos con un ejemplo. Tomemos el número 2351 y sometámoslo a sucesivas divisiones por 5, como se indica a continuación:

2351	5				
35	470	5			
01	20	94	5		
1	0	44	18	5	
		4	3	3	5
				3	0

Veamos cuál es el significado de los sucesivos restos: 3 3 4 0 1 y para ello escribimos

$$2351 = (470 \cdot 5 + 1) = (94 \cdot 5 + 0) \cdot 5 + 1 =$$

$$= 94 \cdot 5^2 + 0 \cdot 5 + 1 = (18 \cdot 5 + 4) \cdot 5^2 + 0 \cdot 5 + 1 =$$

$$= 18 \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5 + 1 = (5 \cdot 3 + 3) \cdot 5^3 +$$

$$+ 4 \cdot 5^2 + 0 \cdot 5 + 1 = 3 \cdot 5^4 + 3 \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5 + 1$$

$$2351 = 3 \cdot 5^4 + 3 \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5 + 1$$

Los restos hallados son los coeficientes de la expresión polinomial en potencias de 5. Puesto que los restos de la división están determinados unívocamente, es posible utilizar esos restos para representar 2351. Entonces escribimos

$$2351 = (33401)_5$$

Se puede cambiar "la base" 5 y obtener análogamente

$$2351 = (100100101111)_2$$

$$2351 = (1848)_{11}$$

9.1. **Teorema.** Sea $s \in N$, $s > 1$. Para todo $n \in N$ existe una expresión polinomial en s, llamada el desarrollo *s-ádico de n,* del tipo siguiente:

$$n = \sum_{i=0}^{t} a_i \cdot s^i, \text{ donde } a_i \in Z, \ 0 < a_i < s$$

Dicho desarrollo es único en el sentido siguiente:

$$\sum_{i=0}^{t} a_i \cdot s^i = \sum_{j=0}^{t} b_j \cdot s^j, \ 0 \leq a_i < s, \ 0 \leq b_j < s$$

$$a_t \neq 0,\ b_h \neq 0$$

implican: $t = h$ y

$$a_i = b_i\ \forall i = 1, \ldots, t$$

Demostración. Si $n = 1$, el desarrollo s-ádico de 1 es 1 y el teorema es trivialmente cierto. Supongamos inductivamente que el teorema ha sido probado para todos los enteros positivos menores que un entero positivo k.

Se debe probar que el teorema es cierto para k. Por el A. D. se tiene

$$k = s \cdot q + r, \quad 0 \leq r < s \qquad [*]$$

Cabe suponer que $s < k$, pues si $k \leq s$, entonces el desarrollo es

$$k = 0 \cdot s + k, \text{ si } k < s$$

$$k = 1 \cdot s + 0, \text{ si } k = s$$

Entonces de $s < k$ y [*] se sigue que $0 < q$. Además, de $1 < s$, se sigue que

76

$$q < q \cdot s \leq q \cdot s + r = k$$

Por lo tanto, por la hipótesis inductiva, el teorema vale para q. O sea

$$q = \sum_{i=0}^{t} a_i \cdot s^i \quad 0 < a_i < s$$

y operando

$$k = q \cdot s + r$$

$$a_t \cdot s^{t+1} + \ldots + a_0 s + r$$

que es un desarrollo s-ádico de k. Por consiguiente, vale el paso inductivo y la primera parte del teorema es cierta cualquiera que sea n. Veamos la unicidad. Sea

$$\sum_{i=0}^{t} a_i \cdot s^i = \sum_{j=0}^{h} b_j \cdot s^j \qquad 0 \leq a_i,\ b_j < s$$

$$a_t \neq 0, \quad b_h \neq 0$$

Entonces

$$a_0 + \left(\sum_{i=0}^{t} a_i \cdot s^{i-1}\right) \cdot s = b_0 + \left(\sum_{j=1}^{h} b_j \cdot s^{j-1}\right) \cdot s$$

Nótese que $a_0 = b_0$ por unicidad del resto en la división por s. Aplicando la hipótesis inductiva a los términos de la derecha en ambos miembros resulta

$$t = h \text{ y } a_1 \ b_1, \ldots, a_t = b_t$$

con lo cual la unicidad queda probada.

8.2 Ejercicios

1. Probar que mediante una balanza de dos platillos y una pesa de cada uno de los valores 1, 2, 4, 8, 16, 32, ... es posible pesar cualquier cuerpo cuyo peso sea un número entero de unidades, y que, además, la forma de hacerlo es única. Demostrarlo para los pesos: 31, 63 y 99.

2. Probar que mediante pesas de 1, 3, 9, 27, 81, ... unidades es posible pesar, y en forma unívoca, cualquier cuerpo cuyo peso sea un número entero de unidades, siempre que sea posible utilizar ambos platillos para colocar pesas.

3. Escribir en el sistema hexadecimal (base 16 y "dígitos" 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) los siguientes números dados en el sistema decimal:

   i) 11, 15, 16, 17, 32, 65, 170, 200, 256, 271,

   ii) 4074, 61.642.

4. Probar que los desarrollos s-ádicos pueden efectuarse para valores de $s < 0$ (**Sugerencia.** Desarrollar en base $-s$ y notar que si $0 \leq t < |s|$, entonces $-t = (|s| - t) + s$. Por ejemplo, en base 5: 17 = $= 2 + 3 \cdot 5 = 2 + (-3)(-5) = 2 + 2 \cdot (-5) + 1 \cdot (-5)^2 = (122)_{-5}$.)

5. i) Escribir en el sistema binario negativo (base -2) los siguientes números dados en el sistema decimal: -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

   ii) Dado $a = (323414)_5$ expresar a y $-a$ en base -5.

   iii) Escribir en el sistema negadecimal (base -10) los siguientes números dados en el desarrollo decimal: -1, -2, -3, 1, 2, 3, 100, 1000, 1234567890. **Ejemplos:** $-1 = (19)_{-10}$, $10 = (90)_{-10}$, $100 = (100)_{-10}$. **Nota.** Obsérvese que si $s > 0$, entonces sólo los números enteros positivos o cero admiten desarrollo en base s. Los números p-ádicos de Hensel permiten desarrollar *todo* entero en base $s > 0$. Por ejemplo, en base $s = 3$,

$$-5 = 1 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^4 + \ldots$$

Una verificación formal de esta igualdad se puede obtener sumando $5 = 2 + 3$ a ambos miembros y "llevándose" unidades en el miembro derecho

$$0 = 3 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^4 + \ldots$$

$$= 0 + 3 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^4 + \ldots$$

$$= 0 + 0 \cdot 3 + 3 \cdot 3^2 + 2 \cdot 3^4 + \ldots$$

$$= 0 + 0 \cdot 3 + 0 \cdot 3^3 + 3 \cdot 3^4 + \ldots$$

......

$$= 0 + 0 \cdot 3 + 0 \cdot 3^2 + 0 \cdot 3^4 + \ldots$$

$$= 0$$

10

PARTE ENTERA Y PARTE DECIMAL DE UN NUMERO REAL

Para cada $a \in R$, existe un número *entero* designado $[a]$ con la propiedad:

$$[a] \leq a < [a] + 1$$

En otras palabras, $[a]$ es el mayor entero menor o igual que a; $[a]$ se llamará *parte entera* de a. El número real $t = a - [a]$, llamado *parte decimal* de a, satisface las propiedades:

$$a = [a] + t \qquad 0 \leq t < 1$$

10.1 Ejemplos

$$[0] = 0, \ [\tfrac{3}{2}] = 1, \ [-\tfrac{3}{2}] = -2,$$

$$[\tfrac{1}{2}] = 0, \ [-\tfrac{1}{2}] = -1, \ [\sqrt{2}] = 1.$$

10.2 Propiedades

i) Si a y b son enteros $a > 0$, entonces existe $r \in Z$ tal que

$$b = a \cdot [\tfrac{b}{a}] + r, \text{ con } 0 \leq r < a.$$

ii) $x \in R$, $n \in Z$; entonces $[x + n] = [x] + n$. En efecto:

$$[x] \leq x < [x] + 1$$

$$[x] + n \leq x + n < [x] + n + 1$$

Y por unicidad de la parte entera: $[x + n] = [x] + n$.

iii) $x, y \in R$, $[x] + [y] \leq [x + y]$. En efecto:

$$[x] \leq x$$

$$[y] \leq y$$

$$[x] + [y] \leq x + y, \text{ o sea } [x] + [y] \leq [x + y].$$

iv)
$$[x] + [-x] = \begin{cases} 0, & \text{si } x \in Z \\ -1, & \text{si } x \notin Z \end{cases}$$

Es claro que si $x \in Z$, entonces $-x \in Z$, de donde $[x] + [-x] = x + (-x) = 0$.

Sea $x \notin Z$. Luego $[x] < x < [x] + 1$; por lo tanto, $-([x]+1) < -x < -[x]$, lo cual dice que $[-x] = -[x] - 1$ y, en consecuencia, $[x] + [-x] = -1$.

v) $[x] + [x + \frac{1}{2}] = [2x]$.

En efecto, sea $x = [x] + \theta$, $0 \leq \theta < 1$. Se sigue que $[x + \frac{1}{2}] = [x] + [\theta + \frac{1}{2}] = x - \theta + [\theta + \frac{1}{2}]$. Por lo tanto, $[x] + [x + \frac{1}{2}] = 2x - 2\theta + [\theta + \frac{1}{2}]$.

Si $0 \leq \theta < \frac{1}{2}$ implica $[\theta + \frac{1}{2}] = 0$, o sea:

$$[x] + [x + \tfrac{1}{2}] \leq 2x = [x] + [x + \tfrac{1}{2}] + 2\theta < [x] + [x + \tfrac{1}{2}] + 1$$

por lo tanto $[2x] = [x] + [x + \frac{1}{2}]$.

Si $\frac{1}{2} \leq \theta < 1$, se tiene $[\theta + \frac{1}{2}] = 1$ y $1 \leq 2\theta < 2$, o sea $2x = [x] + [x + \frac{1}{2}] + 2\theta - 1$, con $0 \leq 2\theta - 1 < 1$; es decir que $[2x] = [x] + [x + \frac{1}{2}]$.

vi) Análogamente se prueba que:

i) $[x] + [x + \frac{1}{3}] + [x + \frac{2}{3}] = [3x]$

y en forma bastante similar la relación general, para todo $m \in N$:

ii) $[x] + [x + \frac{1}{m}] + \ldots + [x + \frac{m-1}{m}] = [mx]$

cuyas demostraciones se dejan como ejercicio para el lector.

vii) Para todo $m \in N$, se tiene $[\frac{x}{m}] = \left[\frac{[x]}{m}\right]$. Sean $x = [x] + \theta$, $0 \leq \theta < 1$; $[x] = ms + t$, $0 \leq t < m$ (algoritmo de división entera). Se tiene:

$$\frac{[x]}{m} = s + \frac{t}{m}, \text{ con } 0 \leq \frac{t}{m} < 1$$

y por lo tanto

$$\left[\frac{[x]}{m}\right] = s$$

Por otra parte, $x = ms + t + \theta$ y como

$$0 \leq t \leq m - 1, \; 0 \leq \theta < 1, \; 0 \leq t + \theta < m$$

de donde $[\frac{x}{m}] = s$. Y en conclusión

$$[\frac{x}{m}] = \left[\frac{[x]}{m}\right]$$

10.3. Una Aplicación Aritmética de $[x]$. Sean $n \in N$, p primo positivo. Entonces el *mayor exponente* m *de* p *tal que* p^m *divide a* $n!$ *es exactamente igual a*

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

(La suma concluye con el primer exponente t tal que $p^t > n$; por ejemplo, $\left[\frac{17}{3}\right] + \left[\frac{17}{3^2}\right] + \left[\frac{17}{3^3}\right] + \ldots = \left[\frac{17}{3}\right] + \left[\frac{17}{3^2}\right] = 5 + 1 = 6.$)

En efecto, los números positivos menores o iguales que n, divisibles por p satisfacen: $p \leq p \cdot t \leq n$

o sea

$$1 \leq t \leq \left[\frac{n}{p}\right] \leq \frac{n}{p}$$

Ahora, los números positivos menores o iguales que n, divisibles por p^2 satisfacen

$$p^2 \leq p^2 \cdot t \leq n, \text{ o sea } 1 \leq t \leq \left[\frac{n}{p^2}\right] \leq \frac{n}{p^2}$$

Este proceso, repetido para todas las potencias de p menores o iguales que n, demuestra nuestra afirmación. Conviene ahora expresar la factorización de $n!$ en producto de primos en la forma siguiente:

$$n! = \prod_{p \in P} p^{\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]}$$

donde P denota la totalidad de primos positivos.

10.4 Ejemplo. El exponente con que 5 aparece en la factorización en producto de primos de 50 ! es

$$\left[\frac{50}{5}\right] + \left[\frac{50}{25}\right] = 10 + 2 = 12$$

Se sigue que el desarrollo decimal de 50 ! termina en 12 ceros. El exponente con que 3 aparece en 50! es

$$\left[\frac{50}{3}\right] + \left[\frac{50}{9}\right] + \left[\frac{50}{27}\right] = 16 + 5 + 1 = 22$$

A manera de ejercicio, halle el lector la factorización en primos de 50!

10.5 Ejemplo. Vamos a determinar el número de ceros en que termina el desarrollo en base 3 de 100! Si $100! = 3^m \cdot b$, con $(b, 3) = 1$, y se escribe $b = 3k + r$, con $r = 1$ o $r = 2$, se tiene:

$$100! = 3^{m+1} \cdot k + r \cdot 3^m$$

lo cual dice que el desarrollo en base 3 de 100! tiene exactamente m ceros. Pero m es la mayor potencia de 3 que divide a 100! Se sabe ya

como calcular esta máxima potencia, o sea mediante la suma

$$[\frac{100}{3}] + [\frac{100}{3^2}] + [\frac{100}{3^3}] + [\frac{100}{3^4}] = 33 + 11 + 3 + 1 = 48$$

En consecuencia, concluimos que el desarrollo en base 3 de 100! termina en 48 ceros.

También es posible determinar el número de ceros en que termina el desarrollo de 100! en base 10 si se halla la mayor potencia de 10 que divide a 100. Puesto que $10 = 2 \cdot 5$, habrá que calcular la mayor potencia de 2 y la mayor potencia de 5 que dividen a 100. De estos dos números habrá que tomar el menor. Por lo tanto habrá que calcular *solamente* la mayor potencia de 5 que divide a 100! Esta es:

$$[\frac{100}{5}] + [\frac{100}{5^2}] = 24$$

Por lo tanto, el desarrollo decimal de 100! termina en 24 ceros. ¿En cuántos ceros termina el desarrollo en base $15 = 3 \cdot 5$ de 100!? La discusión precedente dice que en *24 ceros*.

10.6. Sean $n = p^a$, con p primo positivo, y $a \in N$. Vamos a probar, a manera de ejemplo, que: $n \mid (n-1)!$ si, y sólo si, p es impar y $a > 1$ o $p = 2$ y $a > 2$. Por ejemplo $2^3 \mid 7!$, $3^2 \mid 8!$, $4 \nmid 3!$, $5 \nmid 4!$

Es claro que $p^a \mid (n-1)!$ si, y sólo si, la mayor potencia de p que divide a $(n-1)!$ es por lo menos a. De 10.3 se tiene

$$[\frac{p^a-1}{p}] + [\frac{p^a-1}{p^2}] + \ldots + [\frac{p^a-1}{p^{a-1}}]$$

y de 10.2.ii) la suma precedente es $(p^{a-1}-1) + (p^{a-2}-1) + \ldots + (p-1) = \frac{p^a-1}{p-1} - a$. Hay que analizar la validez de la inecuación

$$\frac{p^a-1}{p-1} - a \geq a, \text{ o sea } p^a - 1 \geq 2a(p-1)$$

Si $p = 2$, la desigualdad es válida para $a > 2$. Si $p \neq 2$, es válida para $a > 1$. La afirmación queda demostrada. Se propone ahora al lector extender este resultado al siguiente: Sean $n \in N$, $n > 4$ y n *compuesto*. Entonces

$$n \mid (n-1)!$$

10.7 Observación. La propiedad 10.2.vii) permite simplificar el cálculo de la suma

$$\sum_{i=1}^{\infty} [\frac{n}{p^i}]$$

En efecto, es de notar que por esa propiedad se tiene

$$[\frac{n}{p^{i+1}}] = \left[\frac{[\frac{n}{p^i}]}{p}\right]$$

Así, por ejemplo, para $n = 1000$ y $p = 3$ los cálculos serían

$$\frac{1000}{3} = 333 + \theta_1, \quad \frac{333}{3} = 111, \quad \frac{111}{3} = 37, \quad \frac{37}{3} = 12 + \theta_2$$

$$\frac{19}{3} = 6 + \theta_3, \quad \frac{6}{3} = 2$$

En consecuencia, la suma buscada es $333 + 111 + 37 + 12 + 6 + 2$.

11

CONGRUENCIAS

Sean $m \in N$ y a y b enteros.

11.1. Definición. Se dice que a es congruente a b, módulo m, en símbolos

$$a \equiv b(m) \text{ o } a \equiv b(\text{mód. } m) \text{ o } a \equiv b, \text{ mód. } m^*$$

si m divide a $b - a$. En símbolos

$$\boxed{a \equiv b(m) \Leftrightarrow m \mid (b - a)}$$

por ejemplo

$1 \equiv -1\ (2)$	$31 \equiv -9\ (10)$
$3 \equiv 1\ (2)$	$13 \equiv 3\ (10)$
$-3 \equiv 1\ (2)$	$121 \equiv 21\ (100)$
$-2 \equiv 7\ (9)$	$4317 \equiv 317\ (1000)$
$2 \equiv -7\ (9)$	$13 \equiv 33\ (10)$
$15 \equiv 0\ (5)$	$131 \equiv 731\ (100)$

Ejemplo. $a \equiv b(1)$ para todo par a, b. Por $a \not\equiv b(m)$ se denota la negación de $a \equiv b(m)$. Por ejemplo

$3 \not\equiv 2\ (2)$ $\qquad$ $5 \not\equiv 4\ (2)$

$3 \not\equiv 0\ (2)$

11.2. Ejercicios

1. Analizar la validez de las siguientes afirmaciones:

i) $11 \equiv -1\ (6)$	v) $31 \equiv -18\ (7)$
ii) $13 \equiv 0\ (2)$	vi) $3 \equiv 3\ (2)$
iii) $10^2 \equiv 10\ (3)$	vii) $1 \equiv -1\ (2)$
iv) $270 \equiv 15\ (54)$	viii) $90 \equiv -1\ (13)$

2. ¿Qué valores de m hacen verdaderas las congruencias siguientes?

i) $5 \equiv 4\ (m)$	iv) $1214567 \equiv 3124567\ (10^m)$
ii) $5 \equiv -4\ (m)$	v) $1 \equiv 0\ (m)$
iii) $1197 \equiv 186\ (m)$	vi) $3 \equiv -3\ (m)$
	vii) $1197 \equiv -286\ (m)$

---

* $a \equiv b$, mód. m, notación original de Gauss, capítulo 1 de *"Disquisitiones Arithmeticae"*

3. Probar que si $a \in Z$ es impar, entonces $a^2 \equiv 1 \ (8)$.

4. Probar, si $a \in Z$, que:

   i) $a^7 \equiv a \ (7)$

   ii) $(a, 7) = 1 \Rightarrow a^6 \equiv 1 \ (7)$.

11.3. Proposición. $\forall a,\ b \in Z,\ a \equiv b \ (m) \Leftrightarrow a$ y b tienen el mismo resto en la división por m.

Demostración. Sean

$$a = m \cdot h + r_a \qquad 0 \leq r_a < m$$

$$b = m \cdot k + r_b \qquad 0 \leq r_b < m, \text{ con } r_a \leq r_b$$

Entonces

$$b - a = m \cdot (k - h) + (r_b - r_a), \text{ con } 0 \leq r_b - r_a < m$$

Se sigue que $r_b - r_a$ es el resto de la división de $b - a$ por m. Por lo tanto

$$\boxed{a \equiv b \ (m) \Leftrightarrow m \mid b - a \Leftrightarrow r_a = r_b}$$

Se deja a cargo del lector verificar las siguientes propiedades de la congruencia:

i) Reflexividad: $a \equiv a \ (m)$.

ii) Simetría: $a \equiv b \ (m) \Rightarrow b \equiv a \ (m)$.

iii) Transitividad: $a \equiv b \ (m)$ y $b \equiv c \ (m) \Rightarrow a \equiv c \ (m)$.

iv) $a \equiv 0 \ (m) \Leftrightarrow m \mid a$.

v) $a \equiv b \ (m) \Rightarrow a + c \equiv b + c \ (m)$.

vi) $a \equiv b \ (m) \Rightarrow ac \equiv bc \ (m)$.

vii) $a \equiv b \ (m)$ y $c \equiv d \ (m) \Rightarrow a \pm c \equiv b \pm d \ (m)$.

viii) $a_i \equiv b_i \ (m),\ i = 1, \ldots, r \Rightarrow \sum_{i=1}^{r} a_i \equiv \sum_{i=1}^{r} b_i \ (m)$.

ix) $a \equiv b \ (m)$ y $c \equiv d \ (m) \Rightarrow ac \equiv bd \ (m)$.

x) $a_i \equiv b_i \ (m),\ i = 1, \ldots, r \Rightarrow \prod_{i=1}^{r} a_i \equiv \prod_{i=1}^{r} b_i \ (m)$.

xi) $a \equiv b \ (m) \Rightarrow a^n \equiv b^n \ (m) \ (n \in N)$.

xii) Sea $f(X) \in Z[X]$ un polinomio con coeficientes enteros, $a \equiv b$ $(m) \Rightarrow f(a) \equiv f(b)$ (m).

xiii) $(m, n) = 1$, $a \equiv b$ (m), $a \equiv b$ $(n) \Rightarrow a \equiv b$ (mn).

xiv) $ab \equiv ac$ $(m) \Rightarrow b \equiv c$ $(\frac{m}{(a, m)})$.

xv) $ac \equiv bc$ $(cm) \Rightarrow a \equiv b$ (m).

xvi) $a \equiv b$ (m) y $n|m \Rightarrow a \equiv b$ (n).

xvii) $a \equiv b$ $(m) \Rightarrow (a, m) = (b, m)$.

xviii) $ac \equiv bc$ (m) y $(c, m) = 1 \Rightarrow a \equiv b$ (m).

(**Nota:** ¿Qué puede decirse de la siguiente afirmación: $ac \equiv bc$ $(m) \Rightarrow$ $\Rightarrow a \equiv b$ (m)? .)

xix) $p > 0$ primo, $ab \equiv 0$ $(p) \Rightarrow a \equiv 0$ (p) o $b \equiv 0$ (p).

xx) **Pequeño Teorema de Fermat:**

- $a^p \equiv a$ (p).
- $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1$ (p).

Es resultado de 4.7.6. y de la propiedad xviii). Otra demostración puede hallarse en 13.8.

11.4. Ejercicios

1. Probar que para todo n, $n^7 - n$ es divisible por 42.
2. Probar que $n^{13} - n$ es divisible por 2, 3, 5, 7, y 13, para todo $n \in N$.
3. Probar que $n^{12} - a^{12}$ es divisible por 13, si n y a son coprimos con 13.
4. Probar que $n^{12} - a^{12}$ es divisible por 91, si n y a son coprimos con 91.
5. Probar que $13 | 2^{70} + 3^{70}$.
6. Probar que $11 \cdot 31 \cdot 61$ divide a $20^{15} - 1$.
7. Probar que si $(a \cdot b, 133) = 1$, entonces $133 | a^{18} - b^{18}$.
8. Probar que para todo n: $2^{2n} \equiv 1$ (3), $2^{3n} \equiv 1$ (7), $2^{4n} \equiv 1$ (15).
9. Probar que si p es un primo mayor que 7, entonces $p^6 - 1$ es divisible por 504.

11.5. **Nota.** Las tres primeras propiedades de $\equiv$ expresan que ésta es una relación de equivalencia en Z. Como tal determina una partición de Z en clases de equivalencias. Una clase de equivalencia está formada por todos los enteros congruentes entre sí, módulo m. Por ejemplo, si m es 5, las clases de equivalencia son exactamente:

$$Z_0 = \{\ldots, -10, -5, 0, 5, 10, \ldots\} = \{5 \cdot k + 0 \mid k \in Z\}$$

$$Z_1 = \{\ldots, -9, -4, 1, 6, 11, \ldots\} = \{5 \cdot k + 1 \mid k \in Z\}$$

$$Z_2 = \{\ldots, -8, -3, 2, 7, 12, \ldots\} = \{5 \cdot k + 2 \mid k \in Z\}$$

$$Z_3 = \{\ldots, -7, -2, 3, 8, 13, \ldots\} = \{5 \cdot k + 3 \mid k \in Z\}$$

$$Z_4 = \{\ldots, -6, -1, 4, 9, 14, \ldots\} = \{5 \cdot k + 4 \mid k \in Z\}$$

La propiedad de ser estas clases una partición de Z significa que

$$Z = Z_0 \cup Z_1 \cup Z_2 \cup Z_3 \cup Z_4$$

$$Z_i \neq \phi \text{ para todo } i = 0, 1, 2, 3, 4$$

$$Z_i \cap Z_j = \phi \text{ si } i \neq j$$

O sea, las clases no son vacías, no tienen elementos en común y su unión es Z.

La propiedad 11.3. es la que caracteriza a la congruencia, y dice que la congruencia módulo m clasifica a los enteros por su resto en la división por m: dos enteros son equivalentes módulo m si, y sólo si, poseen el mismo resto en la división por m. Por ejemplo, si $m = 2$, la clasificación en Z es de pares e impares.

Las propiedades v) y vi) expresan la compatibilidad de la suma y el producto de enteros con respecto a esta relación de congruencia. Esto es muy importante, pues permite "trasladar" las operaciones de suma y producto al conjunto de clases de congruencia. Esto da lugar a los anillos de enteros módulo m y así a la "aritmética módulo m".

11.6. **Aplicación. Criterios de Divisibilidad**

i) Sea a un número natural. Escrito en forma decimal es

$$a = a_r \cdot 10^r + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$0 \leq a_i \leq 9, \quad i = 0, 1, \ldots, r$$

se tiene: $a_0 \equiv a_0 \text{ (mód. 3)/(mód. 9)}$

$$10 \equiv 1 \text{ (mód.3)/(mód. 9)} \Rightarrow a_1 \cdot 10 \equiv a_1 \text{ (mód 3)/(mód. 9)}$$

$$10^2 \equiv 1 \text{ (mód.3)/(mód. 9)} \Rightarrow a_2 \cdot 10^2 \equiv a_2 \text{ (mód. 3)/(mód. 9)}$$

y, en general,

$$\forall n,\ 10^n \equiv 1 \ (\text{mód. } 3)/(\text{mód. } 9) \Rightarrow a_n \cdot 10^n \equiv a_n \ (\text{mód.}3)/(\text{mód.}9)$$

y, por lo tanto (11. 3, vii), sumando miembro a miembro:

$$a \equiv a_0 + a_1 + a_2 + \ldots + a_r \ (\text{mód.}3)/(\text{mód.}9)$$

lo cual dice (según 12. 3) que a y la suma de dígitos $a_0 + a_1 + \ldots + a_r$ del desarrollo decimal de a tienen el mismo resto en la división por 3 (y por 9). De aquí resulta la regla de divisibilidad por 3 (y por 9): un número es divisible por 3 (y, respectivamente, por 9) si, y sólo si, la suma de sus dígitos es divisible por 3 (y por 9, respectivamente).

Ejemplos:

102, 210, 2100, 2001, 2301, son divisibles por 3

27, 270, 72, 720, 702, 7002, son divisibles por 9

ii) Otro caso interesante de estudiar es la divisibilidad por 11. Para ello nos basamos en la congruencia

$$10 \equiv -1 \quad (11)$$

por lo tanto

$$10^2 \equiv 1 \quad (11)$$

$$10^3 \equiv -1 \quad (11)$$

y en general

$$10^n \equiv (-1)^n \quad (11)$$

Si $a = a_r \cdot 10^r + \ldots + a_1 \cdot 10 + a_0$, procediendo como en el caso i) se llega a que

$$a \text{ y } a_0 - a_1 + a_2 \ldots + (-1)^r a_r$$

tienen el mismo resto en la división por 11. Un número es divisible por 11, si la suma alternada de sus coeficientes es divisible por 11.

Ejemplos:

11, 1111, 111111, son divisibles por 11

111, 11111, no son divisibles por 11

2233445566, es divisible por 11.

iii) Criterio de divisibilidad por 7, 11 y 13. Puesto que $1001 = 7 \cdot 11 \cdot 13$, se sigue que

$10^3 \equiv -1$ módulos 7, 11 y 13.

Por lo tanto, dado

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r$$
$$= (a_2 a_1 a_0) + (a_5 a_4 a_3) \cdot 10^3 + \ldots$$

se sigue que el resto de la división de a por 7, o por 11, o por 13, coincide con el mismo resto de

$$a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \ldots$$

Por ejemplo, el número 12. 345. 678. 910 tiene el mismo resto que

$$910 - 678 + 345 - 12 = 565$$

en la división por 7, por 11 y por 13. En consecuencia los números 123. 123, 547. 547 son divisibles por 7, por 11 y por 13. Es de notar que, siendo 7, 11 y 13 coprimos de a dos, el criterio anterior es también un criterio de divisibilidad por 1001.

Se deja como ejercicio para el lector reducir a una fracción irreductible la fracción

$$\frac{547.547}{999.999}.$$

iv) Criterio de divisibilidad por 99. Puesto que $10^2 \equiv 1$ (99), se sigue que si $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots$ tiene el mismo resto en la división por 99 que

$$a_1 a_0 + a_3 a_2 + a_5 a_4 + \ldots$$

Por ejemplo, el número 123. 123 tiene en la división por 99 el mismo resto que

$$23 + 31 + 12 = 66.$$

v) Escribir los números en base 30 y hallar un criterio de divisibilidad por 31. Puesto que $30 \equiv -1$ (31), $30^2 \equiv 1$ (31), etc., se sigue que $(a_r\, a_{r-1} \ldots a_1\, a_0)_{30}$ es divisible por 31 si, y sólo si, $a_0 - a_1 + a_2 - - a_3 + \ldots + (-1)^r a_r$ es divisible por 31.

Ejemplo. Calcular el resto de la división de 7^{122} por 11. Se tiene $122 = 10 \cdot 12 + 2$. Por lo tanto, dado que $7^{10} \equiv 1$ (11)

$$7^{122} \equiv 7^{10.12} \cdot 7^2 \ (11)$$
$$\equiv 7^2 \ (11)$$
$$\equiv 5 \ (11)$$

Luego, el resto buscado es 5.

11.7. **Ejemplo.** Hallar la cifra de las unidades de 17^{15}. Se tiene $17^{15} = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0$. Se trata de hallar a_0, en el desarrollo decimal de 17^{15}. Pero adviértase que a_0 no es otra cosa que la solución de la congruencia

$$17^{15} \equiv a_0 \ (10)$$

Ahora, puesto que $17 \equiv 7 \ (10)$, se reduce a encontrar a_0 tal que

$$7^{15} \equiv a_0 \ (10), \quad 0 \leq a_0 < 10$$

Resulta $7^2 \equiv 9$, $7^3 \equiv 3$, $7^9 \equiv 3^3 \equiv 7$, $7^{12} \equiv 21 \equiv 1$, $7^{15} \equiv 3 \ (10)$.

Luego, $a_0 = 3$.

11.8. **Ejercicios**

1. Enunciar criterios de divisibilidad por: 2, 4, 6, 8, 15, 25, 26.

2. Enunciar criterios de divisibilidad por: 14, 18, 19, 21.

3. Dado que $10^4 \equiv -1 \ (73)$, hallar un criterio de divisibilidad por 73.

4. Hallar criterios de divisibilidad por 3, 5, 7 y 11 en base 2.

5. Hallar criterios de divisibilidad por 8, 7 y 13 en base 12.

6. Hallar un criterio de divisibilidad por 13 en base 1000.

7. Hallar un criterio de divisibilidad por 23 en base 21.

8. Hallar un criterio de divisibilidad por 101 en base 100.

9. Hallar criterios de divisibilidad por 37, 11 en base 1000.

10. Hallar el resto de la división por 7 del número escrito en base 12 con cifras 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b:

$$a9b8a6b543a\,12b0\,12a$$

11. ¿Para qué valores de x es el número $axb83a\,1b75aa$, escrito en base 12, divisible por 7?

12. Justificar el siguiente acertijo. Se toma un número A de tres dígitos (por ejemplo, 927), se lo multiplica por 143 (por ejemplo, $927 \cdot 143 = 132561$). Luego si se multiplican las tres últimas cifras del número así obtenido por 7 se obtiene un número cuyas tres últimas cifras coinciden con A (por ejemplo, $561 \cdot 7 = 3927$) (**Sugerencia.** Obsérvese que $143 \cdot 7 \equiv 1 \ (1000)$).

12

ECUACION LINEAL DE CONGRUENCIA

Se trata de estudiar, en general, el problema de resolución de la ecuación en X

$$a \cdot X \equiv b\ (m) \qquad [*]$$

Es fácil ver que el problema no siempre admite solución; por ejemplo, $2 \cdot X \equiv 3\ (2)$ no posee ninguna solución en Z, pues cualquiera que sea $x \in Z$, $2x \equiv 0\ (2)$ y $3 \equiv 1 \not\equiv 0\ (2)$.

Nótese, además, que si x_0 es solución de [*] también lo es $x_0 + k \cdot m$, de manera que si [*] tiene una solución, tiene entonces infinitas soluciones. Para evitar la ambigüedad de infinitas soluciones, nos limitaremos a considerar las soluciones x de [*] tales que $0 \leq x < m$, que llamaremos soluciones *principales*.

Por ejemplo, la ecuación $3 \cdot X \equiv 7\ (11)$ admite una única solución x, con $0 \leq x < 11$, a saber, $x = 6$.

Se obtienen otras soluciones tomando $x = 6 + k \cdot m$. Por otra parte, si u es también solución de $3 \cdot X \equiv 7$, se tiene $3 \cdot u \equiv 3 \cdot 6 \equiv 7\ (11)$ y, por lo tanto, $3 \cdot (u - 6)$ es múltiplo de 11. Como $11 \nmid 3$ se tiene $11 \mid (u - 6)$, o sea $u - 6 = 11 \times k$, $u = 6 + k \cdot 11$, para algún $k \in Z$.

Se ha probado que la solución general de $3 \cdot X \equiv 7\ (11)$ es $6 + k \cdot 11$, $k \in Z$.

12. 1. $(a, m) = 1$ es condición suficiente para que la ecuación $aX \equiv b\ (m)$ tenga soluciones.

Si $(a, m) = 1$, entonces se sabe que existen enteros r y s tales que

$$1 = r \cdot a + s \cdot m$$

por lo tanto $b = (rb) \cdot a + (sb) \cdot m$ y $a \cdot (rb) \equiv b\ (m)$ con rb solución de [*], lo que prueba el enunciado.

Esta condición no es necesaria; por ejemplo, la ecuación $2 \cdot X \equiv 2\ (4)$ es resoluble (cualquier entero impar la satisface). Sin embargo $(2, 4) = 2 \neq 1$.

12. 2. *La condición necesaria y suficiente para que la ecuación* $a \cdot X \equiv b\ (m)$ *admita una solución es que* $(a, m) \mid b$.

Si x es solución de la ecuación, entonces

$$a \cdot x - b = k \cdot m$$

para algún m, o sea

$$b = a \cdot x + (-k) \cdot m$$

de la cual se sigue que si $a \in Z$ es tal que $d|a$ y $d|m$, entonces $d|b$, por lo tanto $(a, m)|b$.

Recíprocamente, si $(a, m)|b$, al analizar la ecuación

$$\frac{a}{(a, m)} X \equiv \frac{b}{(a, m)} \left(\frac{m}{(a, m)}\right) \qquad [2]$$

se observa que admite solución pues

$$\left(\frac{a}{(a, m)}, \frac{m}{(a, m)}\right) = 1$$

Si x es solución de [2], también lo es de [*], pues se tiene que

$$\frac{a}{(a, m)} x \equiv \frac{b}{(a, m)} \left(\frac{m}{(a, m)}\right) \Rightarrow \frac{a}{(a, m)} x - \frac{b}{(a, m)} = k \cdot \frac{m}{(a, m)} \Rightarrow ax - b =$$

$$= km \Rightarrow ax \equiv b \ (m)$$

Ejercicio. Probar que si x es solución de $aX \equiv b \ (m)$ también lo es de

$$aX \equiv b \left(\frac{m}{(a, m)}\right)$$

12.3. Ejemplo. Sea la ecuación $42 \cdot X \equiv 50 \ (76)$. Como $(76, 42) = 2$ y $2|50$, la ecuación tiene solución.

A partir de la idea anterior de dividir por (a, m), consideremos la ecuación

$$21 \cdot X \equiv 25 \ (38)$$

la cual tiene solución, pues $(38, 21) = 1$. Como

$$42 \cdot X \equiv 50 \ (38)$$

o también

$$4 \cdot X \equiv 12 \ (38)$$

y es claro que $x = 3$ es solución. Por consiguiente, se ha hallado una solución de $21 \cdot X \equiv 25$. Todas las soluciones de $21 \cdot X \equiv 25 \ (38)$ son de la forma $3 + k \cdot 38$.

Volviendo a la ecuación original $42 \cdot X \equiv 50 \ (76)$, obsérvese que

$$3 \text{ y } 3 + 38 = 41$$

son las dos únicas soluciones comprendidas entre 0 y 76.

La solución general de $a \cdot X \equiv b\ (m)$ se obtiene en forma análoga en el caso $(a, m) | b$. Los pasos son:

i) Resolver la ecuación

$$\frac{a}{(a, m)} \cdot X \equiv \frac{b}{(a, m)} \left(\frac{m}{(a, m)}\right)$$

ii) Si x es una solución de la ecuación anterior, $x < \frac{m}{(a, m)}$, las soluciones de $a \cdot X \equiv b\ (m)$ no congruentes entre sí módulo m, son

$$x,\ x + \frac{m}{(a, m)},\ x + 2 \cdot \frac{m}{(a, m)}, \ldots,\ x + ((m, a) - 1) \cdot \frac{m}{(a \cdot m)}$$

o sea, hay (a, m) soluciones no congruentes entre sí módulo m.

12.4. Ejemplo. Sea la ecuación $30 \cdot X \equiv 18\ (78)$. Se tiene $(30, 78) = 6$ y como $6 | 18$ la ecuación tiene solución. Hallemos primeramente una solución de $5 \cdot X \equiv 3\ (13)$. Se ve fácilmente que la solución es 11.

Luego las soluciones de $30 \cdot X \equiv 28$ son

$$11,\ 11 + 13,\ 11 + 2 \cdot 13,\ 11 + 3 \cdot 13,\ 11 + 4 \cdot 13,\ 11 + 5 \cdot 13$$

todas distintas entre sí módulo 78.

12.5. Aplicación. Sean $a, b, c \in N$ con $(a, b) = d$. Se deja como ejercicio para el lector probar que:

i) La ecuación $aX + bY = c$ admite soluciones x_0, y_0 si, y sólo si, $d | c$.

ii) Si x_0, y_0 es solución de la ecuación precedente, entonces la solución general está dada por

$$x = x_0 + h \cdot \frac{b}{d},\quad y = y_0 - h\frac{a}{d}$$

con $h \in Z$ arbitrario.

iii) Resolvamos la ecuación $31X + 21Y = 1770$ en valores de x, y no negativos. Dado que $(31, 21) = 1$, la ecuación admite solución. Se tiene $31 \cdot -2 + 21 \cdot 3 = 1$ y, por lo tanto, $31 \cdot (-2 \cdot 1770) + 21 \cdot (3 \cdot \cdot 1770) = 1770$; con lo que $x_0 = -3540$ e $y_0 = 5310$ son soluciones. Dado que nos interesan soluciones no negativas, hay que resolver las ecuaciones

$$x_0 + h \cdot 21 = -3540 + h \cdot 21 \geq 0$$

$$y_0 - h \cdot 31 = 5310 - h \cdot 31 \geq 0$$

Resulta h: $168,57 \leq h \leq 171,2$, o sea $h \in \{169, 170, 171\}$. Se obtienen las siguientes soluciones:

$h = 169,\ x_1 = 9,\ y_1 = 71;\ h = 170,\ x_2 = 30,\ y_2 = 40;$

$h = 171,\ x_3 = 51,\ y_3 = 9.$

Sean $a,\ b,\ c \in N$ y $(a,\ b) = 1$. Interesa analizar la existencia de soluciones no negativas de la ecuación $ax + by = c$, o sea $x \geq 0,\ y \geq 0$. La resolución de este problema se puede interpretar físicamente si se piensa en recipientes de a litros y b litros y se quiere saber qué capacidad c puede medirse con esos recipientes. Por ejemplo, si $a =$ $= 5$ y $b = 7$ puede medirse:

$$24 = 2 \cdot 5 + 2 \cdot 7 \qquad 28 = 0 \cdot 5 + 4 \cdot 7$$

$$25 = 5 \cdot 5 + 0 \cdot 7 \qquad 29 = 3 \cdot 5 + 2 \cdot 7$$

$$26 = 1 \cdot 5 + 3 \cdot 7 \qquad 30 = 6 \cdot 5 + 0 \cdot 7$$

$$27 = 4 \cdot 5 + 1 \cdot 7 \qquad 31 = 2 \cdot 5 + 3 \cdot 7$$

Es fácil ver inductivamente que cualquier capacidad $c \geq 24$ puede medirse con recipientes de 5 y 7 unidades, respectivamente. En cambio, $c = 23$ no es posible. La condición $(a,\ b) = 1$ asegura que siempre existe solución x_0 e y_0 de la ecuación $ax + by = c$. La solución general es

$$x_0 + t \cdot b,\ y_0 - t \cdot a, \text{ con } t \text{ recorriendo } Z$$

Si se buscan soluciones no negativas, hay que elegir t de manera tal de satisfacer

$$\frac{-x_0}{b} \leq t \leq \frac{y_0}{a}$$

Una condición suficiente para la existencia de un t *entero* en dicho intervalo es que el mismo tenga longitud por lo menos 1, o sea

$$\frac{y_0}{a} - \left(-\frac{x_0}{b}\right) = \frac{y_0}{a} + \frac{x_0}{b} \geq 1$$

es decir

$$\frac{ax_0 + by_0}{a \cdot b} \geq 1$$

o, equivalentemente, $a \cdot b \leq c$.

Por lo tanto, se ha probado que la ecuación $ax + by = c$ tiene soluciones no negativas para todo $c \geq a \cdot b$. **Nota.** La cota $a \cdot b$ puede mejorarse. En el libro *Problems and Theorems in Analysis* de G. Pólya y G. Szegö, Springer, pág. 5 (1976), se demuestra que si $c > a \cdot b - a - b$ existen soluciones no negativas a la ecuación $ax + by = c$. Ese valor: $a \cdot b - a - b + 1$ es óptimo. También se calcula allí el número de soluciones no negativas.

12.6. Ejercicios

1. Hallar todas las soluciones de las ecuaciones lineales de congruencias siguientes:

i) $330\ X \equiv 42\ (273)$.

ii) $35\ X \equiv 14\ (182)$.

iii) $18\ X \equiv 0\ (15)$.

iv) $7\ X \equiv 1\ (11)$.

v) $8\ X \equiv 0\ (13)$.

vi) $10\ X \equiv 2\ (22)$.

vii) $180\ X \equiv -18\ X\ (30)$.

2. Resolver las siguientes ecuaciones de congruencias:

i) $26x \equiv 1\ (17)$.

ii) $29x \equiv 1\ (13)$.

iii) $19x \equiv 1\ (140)$.

iv) $16x \equiv 31\ (1217)$.

v) $7x \equiv 2\ (221)$.

vi) $15x \equiv 28\ (1009)$.

3. Resolver las siguientes ecuaciones lineales de congruencia:

i) $2\ X \equiv 1\ (7)$.

ii) $6\ X \equiv 3\ (21)$.

iii) $111\ X \equiv 25\ (321)$.

iv) $3970\ X \equiv 560\ (2755)$.

v) $18\ X \equiv 30\ (42)$.

vi) $9\ X \equiv 21\ (30)$.

4. En un cine cobran la entrada: \$ 180 a adultos y \$ 75 a menores de edad. En un cierto día se recaudaron \$ 9000 y asistieron más adultos que menores. ¿Cuáles fueron los números posibles de asistentes?

5. Dos productos A y B cuestan, respectivamente, \$ 71 y \$ 83 el kilo. ¿Qué cantidades enteras de ambos pueden comprarse con \$ 1670?

6. Hallar todas las soluciones enteras positivas de la ecuación diofantina $6000 = 39 \cdot X + 54 \cdot Y$.

(**Solución.** Utilizando el A. D. se tiene la relación $3 = 7 \cdot 39 + (-5) \cdot 54$. O sea $6000 = 14000 \cdot 39 + (-10000) \cdot 54$. La solución general resulta de la ecuación $6000 = (14000 - k \cdot \frac{54}{3}) \cdot 39 + (-10000 + k \cdot \frac{39}{3}) \cdot 54$, $k \in Z$.

Las soluciones positivas resultan de las desigualdades:

$$769,23.. = \frac{10000}{13} \leq k \leq \frac{14000}{18} = 777,7..., \text{ o sea } 770 \leq k \leq 777$$

Las soluciones son pues

$$x = 14000 - k \cdot 18, \quad y = -10000 + k \cdot 13$$

con $k = 770, 771, \ldots, 777$).

13

SISTEMAS DE ECUACIONES LINEALES DE CONGRUENCIAS

Sea el sistema

$$x \equiv a_1 \ (m_1), \quad x \equiv a_2 \ (m_2)$$

Se trata de hallar un entero que satisfaga ambas ecuaciones. Por ejemplo, analicemos el sistema

$$x \equiv 3 \ (5) \text{ y } x \equiv 1 \ (6)$$

las soluciones de la primera ecuación son:

$$3,\ 8,\ 13,\ 18,\ 23,\ \ldots$$

y de la segunda son:

$$1,\ 7,\ 13,\ 19,\ 26,\ \ldots$$

se ve entonces que 13 es solución común, luego solución del sistema.

Nótese que si existe solución común, entonces

$$x = a_1 + k \cdot m_1$$

$$x = a_2 + h \cdot m_2$$

de manera que

$$a_1 - a_2 = h \cdot m_2 - k \cdot m_1$$

y así $(m_1, m_2) | a_1 - a_2$.

Recíprocamente, si $(m_1, m_2) | a_1 - a_2$, la ecuación

$$h \cdot m_2 \equiv a_1 - a_2 \ (m_1)$$

admite solución h *(según el resultado del capítulo anterior)* o sea

$$hm_2 - (a_1 - a_2) = tm_1$$

$$a_1 - a_2 = h \cdot m_2 - t \cdot m_1$$

donde

$$x = a_1 + t \cdot m_1 = a_2 + h \cdot m_2$$

es solución del sistema.

Se ha demostrado una parte de la siguiente proposición.

13.1. Proposición. El sistema de congruencias $x \equiv a_1$ (m_1), $x \equiv$ $\equiv a_2$ (m_2) admite solución si, y sólo si, $a_1 - a_2$ es múltiplo de (m_1, m_2). En este caso hay una única solución en el intervalo $0 \leq x < [m_1, m_2]$.

Si $(m_1, m_2) = 1$, el sistema admite siempre solución.

Demostración. Veamos la cuestión relativa a unicidad. Sean x e y con $0 \leq x \leq y < [m_1, m_2]$, soluciones del sistema. Entonces

$$x \equiv y \ (m_1) \text{ y } x \equiv y \ (m_2)$$

Por lo tanto, $y - x$ es divisible por m_1 y por m_2, o sea por $[m_1, m_2]$, pero ello es imposible dado que $0 \leq y - x < [m_1, m_2]$, salvo si $x = y$, en cuyo caso nada queda por probar.

13.2. Ejemplo. Resolvamos el sistema: $3x \equiv 4$ (125), $5x \equiv 3$ (8). Previamente, se convierte en un sistema equivalente al despejar la x. Dado que $3 \cdot 42 = 126 \equiv 1$ (125) y $5 \cdot 5 = 25 \equiv 1$ (8), resulta el sistema

$$x \equiv 4 \cdot 42 \equiv 43 \ (125), \quad x \equiv 15 \equiv 7 \ (8)$$

Por lo tanto

$$x = 43 + 125 \cdot k,$$

$$x = 7 + 8 \cdot t$$

de donde

$$-36 = 125 \cdot k + (-t) \cdot 8$$

o sea

$$-36 \equiv 125 \cdot k \ (8) \text{ o también } 4 \equiv 5 \cdot k \ (8),$$

donde $k = 4$ es solución. Por lo tanto

$$x = 43 + 125 \cdot 4 = 543$$

satisface

$$x \equiv 43 \ (125)$$

$$x = 7 + (-7) + 43 + 125 \cdot 4 =$$

$$= 7 + 36 + 125 \cdot 4 \equiv 7 \ (8).$$

Por lo tanto, 543 es la única solución del sistema en el intervalo $[0, 1000]$.

13.3. Teorema Chino del Resto. Se demostrará un resultado importante, a saber, el Teorema Chino del Resto: Un sistema lineal de congruencias

$$\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ \cdots\cdots\cdots \\ x \equiv a_k \ (m_k) \end{cases}$$

tal que

$$(m_i, m_j) = 1 \text{ si } i \neq j$$

(o sea los módulos son dos a dos coprimos) admite solución única en el intervalo

$$\{t \mid 1 \leq t \leq \prod_{i=1}^{k} m_i\}.$$

Demostración. Sea para cada i: $1, \dots, k$

$$t_i = \frac{\prod_{j=1}^{k} m_j}{m_i} = m_1 \dots \hat{m_i} \dots m_k \text{ (omitir el factor } m_i).$$

Es claro que $(t_i, m_i) = 1$ para todo i. Por lo tanto, existen x_i, $1 \leq x_i < m_i$ tales que $t_i \cdot x_i \equiv 1 \ (m_i)$. El número entero

$$t = a_1 x_1 t_1 + \dots + a_k x_k t_k$$

es evidentemente solución del sistema de congruencias.

Sean $0 \leq t_1 \leq t_2 < \prod m_i$ soluciones del sistema. Entonces, dado que

$$t_2 - t_1 \equiv 0 \ (m_i) \ \forall i = 1, \dots, k \Rightarrow m_i \mid t_2 - t_1$$

se tiene que

$$\prod m_i \mid t_2 - t_1$$

lo cual, dado que $0 \leq t_2 - t_1 < \prod m_i$, sólo es posible si $t_1 = t_2$, con lo cual queda demostrado el teorema.

13.4. **Ejemplo.** Una banda de trece piratas obtuvo un cierto número de monedas de oro, que trataron de distribuir entre sí equitativamente, pero les sobraban 8 monedas. Imprevistamente dos de ellos murieron. Al volver a intentar el reparto, sobraban ahora 3 monedas. Posteriormente, tres de ellos se ahogaron y al intentar distribuir las monedas quedaban cinco. Se trata de saber cuántas monedas había en juego.

Solución. Sea n el número de monedas. Entonces se tiene el sistema

$$n \equiv 8 \ (13)$$
$$n \equiv 3 \ (11)$$
$$n \equiv 5 \ (8)$$

o sea

$$n = 13 \cdot k + 8$$

$$n = 11 \cdot h + 3$$

$$n = 8 \cdot t + 5$$

y así

$$13 \cdot k + 8 \equiv 3\ (11), \text{ o sea } 13 \cdot k \equiv 6\ (11)$$

$$13 \cdot k + 8 \equiv 5\ (8), \text{ o sea } 13 \cdot k \equiv 5\ (8).$$

las soluciones de $13 \cdot k \equiv 6\ (11)$ son

$$3,\ 14,\ \underline{25},\ 36, \ldots .$$

Las soluciones de $13 \cdot k \equiv 5\ (8)$ son

$$1,\ 9,\ 17,\ \underline{25},\ 33, \ldots .$$

Se sigue que 25 es una solución común. Por lo tanto es $n = 25 \cdot 13 + 8 = 333$.

Se tiene, en efecto

$$333 \equiv 8\ (13)$$

$$333 \equiv 3\ (11)$$

$$333 \equiv 5\ (8)$$

habían, pues, 333 monedas.

Resolvamos este ejemplo utilizando el método de demostración del Teorema Chino del Resto. Se tiene

$$t_1 = 88,\ t_2 = 104,\ t_3 = 143$$

Resolviendo las congruencias

$$88\ X \equiv 1\ (13), \text{ o también } 10\ X \equiv 1\ (13)$$

$$104\ X \equiv 1\ (11), \text{ o también } 5\ X \equiv 1\ (11)$$

$$143\ X \equiv 1\ (8), \text{ o también } 7\ X \equiv 1\ (8)$$

o sea $x_1 = 4$, $x_2 = 9$, $x_3 = 7$. Por lo tanto

$$t = 8 \cdot 4 \cdot 88 + 3 \cdot 9 \cdot 104 + 5 \cdot 7 \cdot 143 = 10629 \equiv 333\ (1144).$$

Por lo tanto 333 es la única solución principal.

13.5. Ejercicios

1. i) Hallar el menor $a > 1$, $a \in N$ tal que

$$a \equiv 1\ (4),\ a \equiv 1\ (5),\ a \equiv 1\ (7).$$

ii) ¿Qué enteros poseen restos 1, 2 y 3 al ser divididos, respectivamente, por 3, 4 y 5?

iii) Resolver el sistema de congruencias

$$2\ X \equiv 1\ (5),\ 3\ X \equiv 9\ (6),\ 4\ X \equiv 1\ (7),\ 5\ X \equiv 9\ (11).$$

iv) Hallar un entero que tenga restos 3, 11 y 15 al ser dividido, respectivamente, por 10, 13 y 17.

2. Probar que si $a, b, c, m \in Z$, la ecuación $ax + by + cz = m$ admite soluciones enteras si, y sólo si, $(a, b, c) | m$. Supóngase $(a, b, c) | | m$. Probar que existen enteros t y tales que $(a, b)\ t + cz = m$. Probar, luego, que la ecuación $ax + by = (a, b)t$ admite solución. De esta manera se resuelve la ecuación dada. Resolver la ecuación $48x + 28y + + 16z = 72$.

3. Hallar 4 enteros consecutivos divisibles por 5, 7, 9 y 11, respectivamente.

4. La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informa que la cantidad de huevos recogida es tal que contando de a 3 le sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. El capataz, que estudia aritmética a escondidas, le dice que eso es imposible. ¿Quién tiene razón?

5. Probar que para todo $n > 1$ existen n enteros consecutivos divisibles por cuadrados > 1. (**Sugerencia.** Sean $p_1, \ldots, p_n$ primos positivos distintos dos a dos. Sea el sistema de congruencias $a \equiv \equiv 0\ (p_1^2)$, $a \equiv -1\ (p_2^2)$, $a \equiv -2\ (p_3^2)$, ...).

14

SISTEMA DE RESTOS. FUNCION DE EULER. TEOREMA DE FERMAT

Sea $m > 1$.

14.1. Definición. Se denominará *sistema completo de restos módulo* m a toda sucesión $x_1, \ldots, x_n$ de números enteros tales que *todo* entero es congruente módulo m a uno, y sólo a uno, de los x_i. Ejemplo

i) $0, 1, \ldots, (m - 1)$. módulo m.

ii) $0, 1, 2, 3, 4$

$1, 2, 3, 4, 5$

$10, 11, -12, -13, 144$

son sistemas completos de restos módulo 5.

14.2. Definición. Se denominará *sistema reducido de restos módulo* m a toda sucesión $y_1, \ldots, y_s$ de enteros tales que todo entero *coprimo* con m es congruente módulo m a uno, y sólo a uno, de los y_j. Ejemplo

$1, 2, 3, 4$

$6, 7, 8, 9$

$1, 7, 18, 29$

son sistemas reducidos de restos módulo 5.

Dado m, la totalidad de restos k, $1 \leq k \leq m$, coprimos con m, forma un sistema reducido de restos módulo m. Cualquier otro sistema tiene el mismo número de elementos. Este número se denotará por $\phi(m)$ y da lugar a la conocida función de Euler ϕ. Por ejemplo:

$$\phi(1) = 1,\ \phi(2) = 1,\ \phi(3) = 2,\ \phi(4) = 2,\ \phi(5) = 4,\ \phi(6) = 2,\ \phi(7) = 6.$$

14.3. Proposición. Sea $(a,m) = 1$. Entonces, si $r_1, \ldots, r_m$ es un sistema completo de restos módulo m, así lo es $a \cdot r_1, \ldots, a \cdot r_m$. Análogamente, si $r_1, \ldots, r_{\phi(m)}$ es un sistema reducido de restos módulo m, así lo es $a \cdot r_1, \ldots, a \cdot r_{\phi(m)}$.

Demostración. $a \cdot r_i$ y $a \cdot r_j$ dan el mismo resto en la división por m si, y sólo si, $a \cdot r_i \equiv a \cdot r_j\ (m)$. Puesto que $(a, m) = 1$, esta congruencia equivale a $r_i \equiv r_j (m)$, lo que permite demostrar ambas afirmaciones.

14.4. Proposición. Sea $(a,m) = 1$. Para todo r

$$r,\ r + a,\ r + 2a, \dots,\ r + (m - 1)a$$

es un sistema completo de restos módulo m. Como ejercicio demostrar esta proposición.

14.5. Teorema. Sean $(a,m) = 1$. Entonces, $\phi(a \cdot m) = \phi(a) \cdot \phi(m)$.

Demostración. Considérese el conjunto de números $M = \{q \cdot a + r \mid 0 \le r < a,\ 0 \le q < m\}$. M posee $a \cdot m$ elementos. Además, cada uno de ellos es menor que $a \cdot m$, por lo tanto

$$M = \{j \mid 0 \le j < a \cdot m\}$$

Vamos a determinar el subconjunto de M de elementos coprimos con $a \cdot m$. Puesto que $(a,m) = 1$, es sabido que $(t,\ a \cdot m) = 1$ si, y sólo si, $(t,a) = (t,m) = 1$. Por lo tanto, puede analizarse por separado la coprimalidad respecto de a y de m. Nótese que si r es un resto módulo a coprimo con a, entonces los números

$$r,\ a + r,\ 2a + r, \dots,\ (m - 1) \cdot a + r$$

son todos coprimos con a.

Sea $r_1, \dots, r_{\phi(a)}$ una sucesión reducida de restos módulo a. La sucesión

$$r_1,\ r_1 + a,\ r_1 + 2a, \dots,\ r_1 + (m - 1)a$$

contiene $\phi(m)$ restos coprimos con m, según se infiere de la proposición anterior. Si se hace variar r_1 por los valores $r_1, r_2, \dots, r_{\phi(a)}$, resultará un total de $\phi(a) \cdot \phi(m)$ números $aq + r$, coprimos con a y con m, o sea con $a \cdot m$. Pero como hay $\phi(a \cdot m)$ de tales números $aq + r$, se concluye que $\phi(a \cdot m) = \phi(a) \cdot \phi(m)$. Con lo cual queda demostrado el teorema.

14.6. Proposición. Sean p primo positivo y $n \in N$. Entonces $\phi(p^n) = p^{n-1} \cdot (p - 1)$.

Demostración. Los números positivos menores que p^n y divisibles por p son los que satisfacen $p \le k \cdot p \le p^n$, donde k recorre el intervalo $1 \le k \le p^{n-1}$. O sea hay p^{n-1} enteros t con $1 < t \le p^n$ divisibles por p. Siendo p primo, los restantes números serán coprimos con p y con p^n. O sea $\phi(p^n) = p^n - p^{n-1} = p^{n-1} \cdot (p - 1)$.

14.7. Proposición. Sean $p_1, \dots, p_s$ los divisores primos de m. Se tiene

$$\phi(m) = m \cdot (1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s})$$

Demostración. Se deja como ejercicio (utilizar el T. F. A. y la propiedad anterior). A manera de ejemplo, si $m = 60 = 2^2 \cdot 3 \cdot 5$, se tiene $\phi(60) = \phi(2^2) \cdot \phi(3) \cdot \phi(5) = 2 \cdot 2 \cdot 4 = 16$ y también $\phi(60) = 60 \cdot \frac{1}{2} \cdot$

$\cdot \frac{2}{3} \cdot \frac{4}{5} = 16$. Los números positivos menores de 60 y coprimos con 60 son: 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53 y 59. Es interesante notar que el número 30 es el mayor número con la propiedad de que los números enteros > 1 y menores y coprimos con 30 son todos primos, a saber: 1, 7, 11, 13, 17, 19, 23, 29.

14.8. El Pequeño Teorema de Fermat. Pierre de Fermat (1601-1665), considerado el padre de la teoría de números, nació cerca de Toulouse y pasó toda su vida en el sur de Francia, lejos de los centros europeos importantes. Fermat fue el primer matemático en aceptar el desafío en teoría de números que presentaba la *Aritmética* de Diofanto de Alejandría (325-409), obra editada por primera vez en Europa, en 1621, por Claudio Bachet (1587-1638) en su texto original griego y en una traducción al latín.

Muchos de los resultados de su labor Fermat los comunicaba epistolarmente a sus amigos o los volcaba en notas personales o los escribía en las márgenes de su copia del libro de Bachet. Su hijo Samuel publicó, después de la muerte de Fermat, una segunda edición de la *Aritmética* y agregó las notas marginales (Toulouse, 1670). De estas notas marginales, la más famosa se refiere a una proposición de Diofanto relativa a la descomposición de un cuadrado entero en suma de dos cuadrados. Por ejemplo, $16 = 4^2 = (\frac{16}{5})^2 + (\frac{12}{5})^2$. Este problema está relacionado con la resolubilidad en números naturales x, y y z de la ecuación $x^2 + y^2 = z^2$. Por ejemplo: $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $8^2 + 15^2 = 17^2, \ldots$.

La solución completa de este problema aparece ya en los *Elementos* de Euclides. Es suficiente referirse a ternas x, y y z de números naturales coprimos, es decir sin factores primos comunes. La solución general de $x^2 + y^2 = z^2$ es: $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, donde m y n son números naturales arbitrarios, pero coprimos y de distinta paridad. Fermat escribió en el margen: "en contraste, es imposible descomponer un cubo en suma de dos cubos, una cuarta potencia en suma de dos cuartas potencias y, en general, si $n > 2$ una potencia n-sima en suma de dos potencias n-simas. De esto he descubierto una demostración maravillosa ("demonstrationem mirabilem sane detexi"). El margen es demasiado estrecho para contenerla" (véase el capítulo 1). En otras palabras Fermat afirma la imposibilidad de resolver en números enteros la ecuación (¡diofantina!) $x^n + y^n = z^n$, si n es mayor que 2. Nadie, hasta el presente, ha dado una demostración de esta afirmación, ni tampoco se ha encontrado un $n > 2$ para el cual esta ecuación puede ser resuelta. La afirmación de Fermat se denomina "el Ultimo Teorema de Fermat" o "la Conjetura de Fermat" o "el Gran Teorema de Fermat". Se sabe por métodos computacionales que la conjetura de Fermat es verdadera para todos los n menores que 125.000.

Una de las ocupaciones favoritas de Fermat parece haber sido la de desafiar en la resolución de problemas a otros matemáticos, especialmente a los ingleses, y, muy en particular, a John Wallis. Les proponía problemas, como, por ejemplo: Hallar un cubo tal que la suma de sus divisores positivos sea un cuadrado. Por ejemplo $7^3 + (1 + 7 + 7^2) = 20^2$.

En una carta del 18 de octubre de 1640, Fermat comunicó al matemático Bernard Frénicle de Bessy (1605-1675) el siguiente teorema: si p es un primo y a es cualquier entero coprimo con p, entonces p divide a $a^{p-1} - 1$. Fermat no dio ninguna demostración y fue el gran matemático suizo Leonhard Euler (1707-1783) quien, en 1736, publicó la primer demostración y obtuvo años más tarde, en 1760, una importante generalización.

El resultado enunciado por Fermat constituye el famoso "Pequeño Teorema de Fermat (P. T. F.)", resultado importante y fundamental en muchos aspectos de la teoría de números.

Pequeño Teorema de Fermat: Sea p un número primo positivo y sea a un entero. Entonces

(P. T. F.): $(a,p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Por ejemplo: $2^4 \equiv 1$ (mód.5), $3^{10} \equiv 1$ (mód.11), $2^{16} \equiv 1$ (mód.17)

Una formulación equivalente a la anterior es la siguiente: Sea p primo positivo, a entero. Entonces

(P. T. F.): $a^p \equiv a \pmod{p}$

En efecto, si p divide a a, el enunciado precedente se reduce a $0 \equiv 0$ (mód. p).

Si $p \nmid a$ puede cancelarse un a: $a^{p-1} \equiv 1$ (mód. p). Por ejemplo, $2^5 \equiv$ $\equiv 2$ (mód.5), $4^7 \equiv 4$ (mód.7).

La siguiente es una demostración conceptual del Teorema de Fermat debida a Euler, que aparece en *Disquisitiones Arithmeticae* No. 49.

Sea a un entero coprimo con p, o sea $p \nmid a$. Formemos los $p - 1$ números

$$a,\ 2a,\ 3a, \ldots, (p-1) \cdot a \qquad [1]$$

Se afirma que los restos de la división de esos números por p son exactamente

$$1,\ 2, \ldots, p-1$$

salvo una permutación (o sea son los mismos restos, pero *no* respectivamente). Es decir [1] constituye un sistema completo de restos módulo p. Por ejemplo, si $p = 5$ y $a = 8$ se tienen los números 8, 16, 24, 32 y los restos en la división por 5 son, respectivamente, 3, 1, 4, 2. Para probar la afirmación anterior, nótese que el resto 0 no puede aparecer en la sucesión [1] dado que si $p \mid i \cdot a$, $1 \le i \le p - 1$, entonces $p \mid$ $\mid i$ o $p \mid a$, pero ninguna de las dos cosas puede ocurrir. Además, dos elementos distintos de [1] producen restos distintos. En efecto, si ia y ja producen el mismo resto, con $1 \le i \le j \le p - 1$, entonces $(j - i) \cdot$ $\cdot\, a$ es divisible por p y, por idéntico razonamiento al precedente, se llega a que $j - i$ debe ser 0 o sea $j = i$.

Es claro ahora que

$$a \cdot 2a \cdot 3a \ldots (p-1)a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}$$

es decir

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \ldots (p-1) \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}$$

y por ser $1 \cdot 2 \cdot 3 \ldots (p-1)$ coprimo con p, se puede cancelar en ambos miembros de la congruencia para obtener el P. T. F.: $a^{p-1} \equiv 1$ (mód. p).

Es interesante notar que la recíproca del Teorema de Fermat no es cierta. O sea, dado n natural, con la propiedad de que para todo entero a se verifica que $a^n \equiv a$ (mód. n) no se sigue que n sea primo. En efecto, Carmichael descubrió, en 1909, el menor entero no primo con esa propiedad, a saber $n = 561 = 3 \cdot 11 \cdot 17$. En efecto, dado a entero, habrá que probar que $a^{561} - a$ es divisible por 3, por 11 y por 17. Por aritmética elemental se seguirá que $a^{561} - a$ es divisible por el producto $3 \cdot 11 \cdot 17 = 561$. Debemos, pues, analizar por separado esos casos. Obsérvese que siempre es posible restringirse a los a coprimos con 3, 11 y 17, dado que si, por ejemplo, $3 \mid a$, entonces obviamente $3 \mid a^{561} - a$.

Por Fermat se sabe que

$$a^2 \equiv 1 \text{ (mód.3)}, \text{ o sea } a^{560} \equiv 1 \text{ (mód.3)}, \text{ es decir } a^{561} \equiv a \text{ (mód.3)};$$

$$a^{10} \equiv 1 \text{ (mód.11)}, \text{ o sea } a^{560} \equiv 1 \text{ (mód.11)}, \text{ es decir } a^{561} \equiv a \text{ (mód.11)};$$

$$a^{16} \equiv 1 \text{ (mód.17)}, \text{ o sea } a^{560} \equiv 1 \text{ (mód.17)}, \text{ es decir } a^{561} \equiv a \text{ (mód.17)};$$

por lo tanto, se ha probado nuestra afirmación. Números como 561 se denominan *seudoprimos o números de Carmichael*. Otro ejemplo es $1729 = 7 \cdot 13 \cdot 19$. No se sabe si hay infinitos seudoprimos. Es posible probar que un tal número es necesariamente producto de primos distintos.

El Teorema de Fermat proporciona un criterio bastante efectivo para analizar la no primalidad de un entero positivo n. Es claro que si hay valores $0 < a < n$ tales que $a^{n-1} \not\equiv 1$ (mód. n), entonces n no es primo. Precisamente este criterio sirve para probar la no primalidad del número de Fermat $2^{2^5} + 1$. En una carta que escribió en 1640 al monje francés Marin Mersenne, Fermat conjeturaba la primalidad de números de la forma $2^{2^m} + 1$, pero decía que en el caso de $m = 5$ no podía probarlo. ¡Fue en ese mismo año que Fermat enunció su teorema! El número $2^{32} + 1$ tiene diez cifras decimales, es, en efecto, $2^{32} + 1 = 4294967297$.

Podemos calcular $3^{2^{32}}$ elevando 32 veces al cuadrado: 3^2, $(3^2)^2$, $((3^2)^2)^2, \ldots$ para obtener, módulo $2^{32} + 1$, el valor 3029026160, lo cual indica que $2^{32} + 1$ *no* es primo. Fue Euler quien probó la no primalidad de $2^{32} + 1$ al descubrir que 641 era divisor de este número. Se deja a cargo del lector llevar a cabo esta verificación a partir de la siguiente expresión: $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$.

Veamos ahora algunos ejemplos de aplicación del P. T. F.

14.9. Ejemplos.

1. Hallar el resto de la división de 47^{7385} por 17. Según el P. T. F. se tiene que, si $17 \nmid a$, $a^{16} \equiv 1$ (mód. 17). Por lo tanto, se divide 7385 por 16 y resulta $7385 = 461 \cdot 16 + 9$. En consecuencia

$$47^{7385} \equiv 13^{7385} \equiv 13^9 \equiv (-4)^9 = -4^9$$

Puesto que $4^2 \equiv -1$ (mód. 17), se sigue que $4^9 = 4^8 \cdot 4 = 1 \cdot 4 = 4$ (mód. 17). En definitiva

$$47^{7385} \equiv -4 \equiv 13 \text{ (mód. 17)}$$

y el resto buscado es 13.

2. Hallar el resto de la división de 3^{1037} por 61. En forma análoga al ejemplo 1, se efectúa la división $1037 = 16 \cdot 60 + 17$ y se tiene

$$3^{1037} \equiv 3^{17} \text{ (mód. 61)}$$

Se tiene, además, que $3^4 \equiv 20$ (mód. 61), por lo tanto $3^5 \equiv 60 \equiv -1$ (mód. 61), o sea $3^{15} \equiv -1$ (mód. 61), $3^{17} \equiv -3^2 \equiv 52$. El resto buscado es 52.

3. Hallar el resto de la división de 3^{1037} por 17. Se deja a cargo del lector verificar que el resto es 12.

4. Hallar el resto de la división de 3^{1037} por $1037 = 61 \cdot 17$. Esta situación se resuelve a partir de los ejemplos 2 y 3. Se trata de hallar el resto de 3^{1037} en la división por 1037 conociendo los restos en la división por 61 y 17. En términos de congruencia, el problema se plantea por el sistema de ecuaciones

$$\begin{cases} X \equiv 12 \text{ (mód. 17)} \\ X \equiv 52 \text{ (mód. 61)} \end{cases}$$

Escribamos, utilizando el algoritmo de división, $1 = 18 \cdot 17 - 5 \cdot 61$. Se verifica que $1 \equiv 18 \cdot 17$ (mód 61) y $1 \equiv -5 \cdot 61 \equiv 12 \cdot 61$ (mód 17); por lo tanto, si escribimos

$$x = 52 \cdot 18 \cdot 17 + 12 \cdot 12 \cdot 61$$

se ve inmediatamente que x satisface las dos ecuaciones precedentes. Debemos hacer una reducción módulo 1037. Se tiene

$$x = 15912 + 8784 \equiv 357 + 488 = 845$$

y éste es el resultado buscado. Nótese que el número 3^{1037} tiene *495 cifras* decimales, lo cual hace imposible cualquier tipo de manipuleo directo de este número.

Resolver la ecuación $8X^{60} + X^{50} + 3X^{25} \equiv 0$ (mód. 13). Es claro que $x \equiv 0$ (mód. 13) es solución. Busquemos soluciones no divisibles por 13. Dado que entonces $x^{12} \equiv 1$ (mód. 13), la ecuación anterior se reduce a $X^2 + 3X + 8 \equiv 0$ (mód. 13). Se trata, pues, de una ecuación de segundo grado.

Su discriminante es $3^2 - 4 \cdot 8 = 9 - 32 \equiv 9 - 6 = 3$ (mód. 13). Como $4^2 \equiv 3$ (mód. 13) resulta $3^2 - 4 \cdot 8 \equiv 4^2$ (mód. 13) y las soluciones de la ecuación dada son, módulo 13,

$$x = \frac{-3 \pm 4}{2} = 7 \cdot (-3 \pm 4) = 7,\ 3$$

6. El número de Mersenne $2^{11} - 1$ no es primo. En efecto, se sigue del teorema de Fermat que $2^{22} \equiv 1$ (23), por lo tanto

$$(2^{11} - 1) \cdot (2^{11} + 1) \equiv 0 \ (23)$$

y entonces

$$2^{11} - 1 \equiv 0 \ \text{ó} \ 2^{11} + 1 \equiv 0 \ (23)$$

Verifiquemos que $2^{11} - 1 \equiv 0$ (23), lo cual probará que $2^{11} - 1$ es divisible por 23 y, por lo tanto, no puede ser primo. Se tiene

$$2^{11} = 2 \cdot 2^5 \cdot 2^5 \equiv 2 \cdot 9 \cdot 9 \equiv 2 \cdot 12 \equiv 1 \ (23)$$

Mediante un razonamiento análogo se prueba que el número de Mersenne $2^{23} - 1$ no es primo. Los detalles de la demostración se dejan a cargo del lector.

Obsérvese que el razonamiento no se aplica al número $2^{29} - 1$, que no es primo.

14.10. Teorema de Euler-Fermat. La generalización del P. T. F. hecha por Euler se hace para todo $n \in N$ mediante la llamada *función de Euler* $\phi(n)$

$$\phi(n) = \text{número de enteros } k \text{ tales que } 1 \leq k \leq n \ \text{ y } \ (n, k) = 1$$

Por ejemplo

$\phi(1) = 1$ $\phi(2) = 1$ $\phi(3) = 2$ $\phi(4) = 2$ $\phi(5) = 4$ $\phi(6) = 2$

$\phi(7) = 6$ $\phi(8) = 4$ $\phi(9) = 6$ $\phi(10) = 4$ $\phi(11) = 10$ $\phi(12) = 4$

Adviértase que si p es primo positivo, entonces $\phi(p) = p - 1$.

El Teorema de Euler (también llamado de Euler-Fermat) establece que si n es natural, entonces para todo entero a, coprimo con n, se verifica

$$a^{\phi(n)} \equiv 1 \ (\text{mód.} \, n)$$

Si, en particular, $n = p$ es primo, se tiene $\phi(p) = p - 1$ y se obtiene el teorema de Fermat. La demostración de este resultado es enteramente análoga a la del teorema de Fermat. Si $(a, n) = 1$ y

$$r_1, \ldots, r_{\phi(n)}$$

es la totalidad de restos positivos módulo n, *coprimos con* n, entonces

$$a \cdot r_1, \ldots, a \cdot r_{\phi(n)}$$

producen exactamente los mismos restos. Por lo tanto

$$\Pi_i r_i \equiv \Pi_i \, a \cdot r_i \pmod{n}$$

$$\Pi_i r_i \equiv a^{\phi(n)} \cdot \Pi_i r_i \pmod{n}$$

y cancelando $\Pi_i r_i$ resulta $a^{\phi(n)} \equiv 1 \pmod{n}$.

A manera de ejemplo de aplicación del Teorema de Euler se calcularán las tres últimas cifras del desarrollo decimal del número 7^{9999}, que tiene 8451 cifras. Si se escribe

$$7^{9999} = a_k \cdot 10^k + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$0 \leq a_i < 10$$

se trata de calcular los tres dígitos a_2, a_1 y a_0, o sea el número $a_2a_1a_0$. Es claro que $a_2a_1a_0$ no es otra cosa que el entero a que satisface

$$\begin{cases} 7^{9999} \equiv a \pmod{1000} \\ 0 \leq a < 1000 \end{cases}$$

Calculemos $\phi(1000)$. Se tiene

$$\phi(1000) = \phi(5^3 \cdot 8) = \phi(5^3) \cdot \phi(8) = 25 \cdot 4 \cdot 4 = 400$$

Se sigue del Teorema de Euler que $7^{400} \equiv 1 \pmod{1000}$. Por lo tanto, dado que $9999 = 400 \cdot 24 + 399$, se tiene

$$7^{9999} \equiv (7^{400})^{24} \cdot 7^{399} \equiv 7^{399} \pmod{1000}$$

Como $7^{400} \equiv 1 \pmod{1000}$, se sigue que $1 \equiv 7^{399} \cdot 7 \pmod{1000}$, y se debe resolver la ecuación $7 \cdot X \equiv 1 \pmod{1000}$ o equivalentemente la ecuación $7 \cdot X \equiv 1001 \pmod{1000}$. Pero 1001 es divisible por 7: $1001 = 7 \cdot 143$. Por lo tanto, $X = 143$. Se concluye que

$$7^{9999} \equiv 7^{399} \equiv 143 \pmod{1000}$$

El desarrollo decimal de 7^{9999} termina en 143.

14.11. Ejercicios

1. Obtener los restos de la división de 2^{46}, 3^{21}, 7^{126}, 99^{99} por 47, 17, 123 y 13, respectivamente.

2. Hallar todos los números que satisfacen, en cada caso:

i) $x^2 \equiv 1$ (4). iv) $x^2 \equiv 0$ (12).

ii) $x^2 \equiv x$ (12). v) $x^4 \equiv 1$ (16).

iii) $x^2 \equiv 2$ (3). vi) $x^2 \equiv -1$ (13).

3. Resolver las siguientes ecuaciones de congruencias:

i) $3x \equiv 1$ (5). iv) $5x \equiv 6$ (7).

ii) $2x \equiv 3$ (6). v) $3x \equiv 2$ (2).

iii) $2x \equiv 5$ (6). vi) $7x \equiv -1$ (8).

4. Probar que ningún entero de la forma $a = 4 \cdot 14^k + 1$, $k \geq 1$ es primo (**Sugerencia.** k impar $\Rightarrow 3 \mid a$, k par $\Rightarrow 5 \mid a$).

5. Hallar los $a \in Z$ para los que la ecuación $ax \equiv 11^{256}$ (13) tiene por solución principal a 8.

6. Sea p primo > 0. Probar que $a \equiv b(p) \Rightarrow a^p \equiv b^p$ (p^2).

7. Sean p y q primos distintos positivos. Probar que $p^{q-1} + q^{p-1} \equiv$ $\equiv 1$ $(p \cdot q)$.

8. Sean a y b enteros positivos coprimos. Probar que mediante recipientes de a litros y b litros es posible medir cualquier cantidad entera de litros.

9. Sea p, primo > 0 impar. Probar:

i) $\sum_{i=1}^{p-1} i^p \equiv 0$ (p), ii) $\sum_{i=1}^{p-1} i^{p-1} \equiv -1$ (p).

10. Hallar en su desarrollo decimal:

i) la cifra de las unidades de 7^{83}.

ii) las dos últimas cifras de 17^{15}.

iii) las dos últimas cifras de 3^{400}.

11. Probar que si $(a, 1001) = 1$, entonces $1001 \mid a^{720} - 1$.

12. Sea n impar. Probar que $n \mid 2^{n!} - 1$

13. Sabiendo que $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$, deducir que el número de Fermat $2^{32} + 1$ no es primo.

14. Sea $p \in N$, $p \geq 2$. Probar que p es primo si, y sólo si, $(p-1)! \equiv$ $\equiv -1$ (p) *(Teorema de Wilson)*. (**Sugerencia.** ($\Rightarrow$). Por Fermat, $x^p - x \equiv$ $\equiv x(x-1)(x-2) \ldots (x-(p-1))$ en el anillo de polinomios $Z_p[x]$.)

15. Sea p primo > 0, impar.

i) Sea $1 \leq k < p$. Probar que $k^2 \equiv 1$ si, y sólo si, $k \equiv 1$ ó -1 (p).

ii) Sean k, t, $1 \leq k, t < p$. Probar que si $k \not\equiv 1$ ó -1 (p), entonces $k \cdot t \equiv 1$ implica $k \neq t$.

iii) Probar mediante i) e ii) el *Teorema de Wilson:* $(p - 1)! \equiv -1\,(p)$.

16. Hallar el resto de la división de $2 \cdot (26!)$ por 29.

17. Yeti. Probar que $28! + 233$ es divisible por 899.

18. Sea p un primo > 0 de la forma $4m + 1$. Probar, mediante el Teorema de Wilson, que la ecuación $x^2 \equiv -1\,(p)$ es resoluble en Z. Se dice entonces que -1 es *residuo cuadrático* módulo p. Resolver la ecuación en el caso de $p = 13$, 17, 29 y 37.

19. Probar que la ecuación $x^2 \equiv -1\,(11)$ no admite solución en Z.

20. Probar que $11 | a^2 + 5b \Leftrightarrow 11 | a$ y $11 | b$.

21. Mostrar un sistema reducido de restos módulo 7 formado por potencias de 3. (Se dice entonces que 3 es una *raíz primitiva* módulo 7.) ¿Es 3 raíz primitiva módulo 17?

22. Sea p primo impar. Probar que los enteros $-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}$ es un sistema reducido de restos módulo p.

23. Probar que $2, 2^2, 2^3, \ldots, 2^{18}$ forman un sistema reducido de restos módulo 27.

24. Probar que para ningún $a \in N$ es a, a^2, a^3, a^4 un sistema reducido de restos módulo 8.

25. Sea $n \in N$, $n > 2$. Probar que $\phi(n)$ es par.

26. Probar que si $n \in N$, $n \geq 2$, la suma de los restos k, $1 \leq k < n$, coprimos con n, es $\frac{1}{2} \cdot n \cdot \phi(n)$. (**Sugerencia.** $1 = (k, n) \Leftrightarrow (n - k, n) = 1$.)

27. Sea $n \in N$. Probar las afirmaciones:

i) n impar $\Rightarrow \phi(2n) = \phi(n)$.

ii) n par $\Rightarrow \phi(2n) = 2\phi(n)$.

iii) $3 | n \Rightarrow \phi(3n) = 3\phi(n)$.

iv) $3 \nmid n \Rightarrow \phi(3n) = 2\phi(n)$.

v) $\phi(n) = \frac{n}{2}$ si, y solo si, $n = 2^k$, $k \geq 1$.

28. Sean n, m en N. Probar

i) $n|m \Rightarrow \phi(n)|\phi(m)$.

ii) $(n,m) \cdot \phi(n) \cdot \phi(m) = \phi(n \cdot m) \cdot \phi((n,m))$.

iii) $\phi(n) \cdot \phi(m) = \phi((n,m)) \cdot \phi([n,m])$.

29. i) Hallar todas las soluciones de $\phi(n) = 8$, $\phi(n) = 6$, $\phi(n) = 10$, $\phi(n) = 16$, $\phi(n) = 17$.

ii) Probar que para todo k existen a lo sumo un número finito de soluciones de la ecuación $\phi(n) = k$.

iii) *Conjetura de Carmichael.* Para todo k, $\phi(n) = k$ tiene por lo menos dos soluciones o ninguna solución.

30. Sean p primo impar y $a \in N$ con $(a,p) = 1$. Probar que la ecuación $x^2 \equiv a$ (p) tiene solución si $a^{\frac{p-1}{2}} \equiv 1$ (p) y no tiene solución si $a^{\frac{p-1}{2}} \equiv -1$ (p). (**Sugerencia.** Nótese que $x^{\frac{p-1}{2}} \equiv 1$ (p) admite por soluciones no congruentes entre sí a: $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$. Estas son todas las soluciones de $x^{\frac{p-1}{2}} - 1 \equiv 0$ (p) razonando en el anillo de polinomios $Z_p[x]$, con Z_p el cuerpo de restos módulo p). Deducir que si p es primo impar, entonces -1 es residuo cuadrático si, y sólo si, p es de la forma $4k+1$.

31. Sea p un primo positivo de la forma $4m+1$. Probar que p es suma de dos cuadrados. (Sugerencia. La hipótesis implica que -1 es residuo cuadrático módulo p o sea $p|x^2+y^2$. Por un resultado anterior, p es suma de dos cuadrados.) Probar que un primo $p > 0$ impar es suma de dos cuadrados si, y sólo si, p es de la forma $4m+1$.

32. Sea p un primo de la forma $4m+3$. Probar que $p|x^2+y^2 \Rightarrow$ $\Rightarrow p|x$ y $p|y$.

14.2. Aplicación del Teorema de Fermat. Z_p^* es un grupo cíclico. Sean p primo y Z_p el anillo de restos módulo p. Por ser p primo, Z_p es un cuerpo. Denótese por Z_p^* la totalidad de elementos de Z_p distintos de cero. Es claro que Z_p^* es un grupo de orden $p-1$. Se probará en esta sección la existencia de elementos $a \in Z_p^*$ con la propiedad de generar todo Z_p^*, o sea, todo elemento es una potencia de a. Por ejemplo, si $p = 5$, $a = 2$ en Z_5^* tiene esa propiedad: $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1$. Podemos, sin pérdida de generalidad, restringirnos al caso $p \neq 2$. Recordaremos algunos conceptos básicos de la teoría de grupos. Sea G un grupo y $a \in G$. Si $a^t = 1$ (1 denota el elemento neutro de G), $t \in N$, se dice que a tiene orden finito. El mínimo t se denota por $o(a)$ y se denomina el *orden* de a. Las propiedades de $o(a)$ son las siguientes: $a^{o(a)} = 1$, $a^r \neq 1$ si $1 \leq r < o(a)$. Se deja como ejercicio la demostración de las siguientes dos propiedades relevantes:

i) Si a tiene orden finito, entonces $a^t = 1$, $t \in N \Rightarrow o(a)$ divide a t.

ii) Si $a, b \in G$ tienen ambos orden finito y además $a \cdot b = b \cdot a$, entonces $a \cdot b$ tiene orden finito $o(a \cdot b) = [o(a), o(b)]$.

Ambas propiedades se siguen de consideraciones puramente aritméticas. De acuerdo con el teorema de Fermat, $a \in Z_p^*$ satisface $a^{p-1} = 1$. Por lo tanto, se sigue de i) que $o(a) | p - 1$, cualquiera que sea a en Z_p^*.

14.12.1. Proposición. Sea $p \geq 3$, q primo y $t \in N$ tal que $q^t | p - 1$. Existe entonces en Z_p^* un elemento de orden q^t.

Demostración. La ecuación $x^{\frac{p-1}{q}} = 1$ tiene a lo sumo

$$\frac{p-1}{q} \leq \frac{p-1}{2} \leq p - 2$$

soluciones en Z_p dado que Z_p es un cuerpo (¡sobre un cuerpo un polinomio de grado n tiene a lo sumo n raíces!).

Por lo tanto, para algún c en Z_p^*, $c^{\frac{p-1}{q}} \neq 1$. Sea $a = c^{\frac{p-1}{q^t}}$. Es claro $a^{q^t} = 1$. Veamos que el orden de a es exactamente q^t. Puesto que $o(a) | q^t$ según i) y siendo q primo, se concluye que $o(a) = q^h$, $1 \leq h \leq t$. Si $h < t$, entonces $a^{q^{t-1}} = 1$, es decir $c^{\frac{p-1}{q}} = 1$ es un absurdo y provino de suponer $h < t$. Es, entonces, $o(a) = q^t$, con lo cual queda demostrada la proposición.

14.12.2. Proposición. Z_p^* es cíclico.

Demostración. Si $p - 1 = q^t$ para algún primo q, la proposición se sigue de la precedente. Si $p - 1 = q_1^{t_1} \ldots q_r^{t_r}$, $r > 1$, se procede inductivamente a partir de la propiedad ii).

Definición. Los elementos $a \in Z_p^*$ se denominan *raíces primitivas módulo p*. En general, cualquier entero a tal que su resto módulo p sea una raíz primitiva módulo p se denomina raíz primitiva módulo p.

14.13.3. Ejemplo. Raíces primitivas mínimas de los primos menores que 100.

p	raíz	p	raíz	p	raíz	p	raíz	p	raíz
2	1	13	2	31	3	53	2	73	5
3	2	17	3	37	2	59	2	79	3
5	2	19	2	41	6	61	2	83	2
7	3	23	5	43	3	67	2	89	3
11	2	29	2	47	5	71	7	97	5

14.14. Problema. Obtener el Teorema de Wilson a partir de la existencia de raíces primitivas. Sea p primo positivo: el Teorema de Wilson establece que $(p - 1)! \equiv -1\ (p)$. En términos de la teoría de grupos significa que el producto de todos los elementos de Z_p^* es -1 (o sea $p - 1$). Sea a raíz primitiva módulo p. Los elementos $1, a^1, a^2, a^3, \ldots, a^{p-2}$ son todos distintos en Z_p^*. Por lo tanto, coinciden, salvo una permutación, con $1, 2, \ldots, (p - 1)$. Se sigue que

$$(p - 1)! = \prod_{i=0}^{p-2} a^i = a^{\frac{(p-1)(p-2)}{2}} = \left(a^{\frac{p-1}{2}}\right)^{p-2}$$

Pero siendo a raíz primitiva

$$a^{\frac{p-1}{2}} = -1$$

Se concluye que $(p - 1)! = -1$ en Z_p, o sea $(p - 1)! \equiv -1\ (p)$.

14.15. Símbolo de Legendre y Criterio de Euler. Sea p un número primo impar y positivo. Para todo $a \in Z$, $(a, p) = 1$ se define el símbolo de Legendre

$$\left(\frac{a}{p}\right) := \begin{cases} 1 \text{ si } a \text{ es residuo cuadrático módulo } p \\ -1 \text{ si } a \text{ no es residuo cuadrático módulo } p \end{cases}$$

es decir, según tenga o no solución en Z la ecuación de congruencia $x^2 \equiv$ 117
$\equiv a\ (p)$. Por ejemplo, $\left(\frac{2}{3}\right) = -1$, $\left(\frac{-1}{5}\right) = 1$, $\left(\frac{12}{7}\right) = \left(\frac{5}{7}\right) = -1$.

Sabemos que, según el teorema de Fermat, $a^{p-1} \equiv 1\ (p)$, si $(a, p) = 1$. Por lo tanto, $(a^{\frac{p-1}{2}} - 1) \cdot (a^{\frac{p-1}{2}} + 1) \equiv 0\ (p)$, es decir $a^{\frac{p-1}{2}} \equiv 1$ ó $a^{\frac{p-1}{2}} = -1$, módulo p. El criterio de Euler permite decidir cuál de esos casos ocurre. (Adviértase que por ser p primo impar, la ocurrencia simultánea no es posible.)

Criterio de Euler. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{b}\right)\ (p)$.

Demostración. Sea c una raíz primitiva módulo p. Entonces $a \equiv c^t\ (p)$ para algún entero positivo t. Por ser c raíz primitiva, es claro que $c^{\frac{p-1}{2}} \equiv (-1)\ (p)$, por lo tanto

$$a^{\frac{p-1}{2}} \equiv c^{t \cdot \frac{p-1}{2}} \equiv \left(c^{\frac{p-1}{2}}\right)^t \equiv \begin{cases} 1, \text{ si } t \text{ es par} \\ -1, \text{ si } t \text{ es impar} \end{cases}$$

o sea $\equiv 1$ si a es un cuadrado módulo p y $\equiv -1$ si no lo es. El criterio queda demostrado.

Corolario. Sean a, b enteros coprimos con p. Entonces

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

(carácter multiplicativo del símbolo de Legendre).

Mencionemos finalmente la famosa *ley de reciprocidad cuadrática:* Sean p y q primos positivos impares y distintos. Entonces

$$\text{(LRC):}\quad \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

o sea, hay una relación entre la propiedad de ser q residuo cuadrático módulo p y la de ser p residuo cuadrático módulo q.

APENDICE I. PRINCIPIO DE INDUCCION

Sea $N := \{1, 2, 3, \ldots\}$ el conjunto de números naturales. En este Apéndice nos limitaremos a ejemplificar una de las propiedades fundamentales de los números naturales, a saber: la validez del principio de inducción o recurrencia y sus formulaciones equivalentes. Para ello se consignarán tres de las formas más simples del principio y sus interpretaciones, que facilitan la demostración general de numerosos resultados matemáticos.

1. Principio de Inducción

a) Sea $N = (1, 2, 3, \ldots)$ el conjunto de los números naturales y P un subconjunto de N (o sea $P \subset N$) tal que:

i) 1 pertenece a P.

ii) Si k pertenece a P, entonces $k + 1$ pertenece a P.

Entonces, P es el conjunto de los números naturales.

En símbolos:

$$P \subset N \text{ y } \left.\begin{array}{l} \text{i) } 1 \in P \\ \text{ii) } k \in P \Rightarrow k + 1 \in P \end{array}\right\} \Rightarrow P = N$$

donde por $\Rightarrow$, símbolo de implicación, sólo se quiere expresar que si el antecedente es verdadero el consecuente también lo es.

b) Sea P un subconjunto de N tal que:

i) 1 pertenece a P.

ii) Si, cualquiera que sea $n \in N$, todos los números k menores que n pertenecen a P, entonces n pertenece a P.

Entonces, P es el conjunto N de los números naturales.

En símbolos:

$$\text{Sea } P \subset N \text{ y } \left.\begin{array}{l} \text{i) } 1 \in P \\ \text{ii) } \forall n\, (\forall k \in N,\ k < n \Rightarrow k \in P) \Rightarrow n \in P \end{array}\right\} P = N$$

c) Sean $P \subset N$ y $p \in N$ tales que

i) $p \in P$

ii) $k \geq p$ y $k \in P \Rightarrow k + 1 \in P$.

Entonces, P contiene todos los números naturales $k \geq p$.

2. Utilización del Principio de Inducción

a) Sean $P(n)$ una proposición predicable sobre N, es decir: para cada $n \in N$, $P(n)$ designa una proposición verdadera o falsa tal que:

i) $P(1)$ es verdadera.

ii) Para todo $k \in N$, si $P(k)$ es verdadera, entonces $P(k + 1)$ es verdadera.

Entonces, $P(n)$ es verdadera *cualquiera* que sea $n \in N$.

b) Sea $P(n)$ tal que:

i) $P(1)$ es verdadera.

ii) Para todo $n \in N$, si $k < n$ $P(k)$ es verdadera, entonces $P(n)$ es verdadera.

Entonces, $P(n)$ es verdadera para todo $n \in N$.

c) Sea $P(n)$ tal que:

i) $P(p)$ es verdadera.

ii) Para todo $k \geq p$, si $P(k)$ es verdadera, entonces $P(k + 1)$ es verdadera.

Entonces, $P(n)$ es verdadera cualquiera que sea $n \geq p$.

3. Ejemplos

a) Probemos que 64 divide a $7^{2n} + 16n - 1$ para todo $n \in N$. Debemos probar que se cumplen 2. a. i) y 2. a. ii).

i) Si $n = 1$, la afirmación es verdadera.

ii) Supongamos que la propiedad es cierta para n y, basados en ello, probemos que es cierta para $n + 1$. En efecto,

$$7^{2(n+1)} + 16(n + 1) - 1 = (7^{2n} + 16n - 1) \cdot 7^2 - 16 \cdot 7^2 \cdot n + $$
$$+ 7^2 + 16n + 16 \cdot 1$$
$$= (7^{2n} + 16n - 1) - 16 \cdot n \cdot (7^2 - 1) + 64$$

El primer término es múltiplo de 64 por la hipótesis inductiva ii) (para n) y resulta

$$7^{2(n+1)} + 16(n + 1) - 1 = \text{mult. } 64.$$

Hemos probado que $P(n)$ es cierta para $n + 1$, cuando lo es para n, por tanto, $P(n)$ resulta cierta para todo n.

b) Sea $f: N \to N$ la aplicación definida por

$$f(n) = \begin{cases} n/2 & \text{si } n \text{ es par} \\ n+3 & \text{si } n \text{ es impar} \end{cases}$$

Se trata de analizar el comportamiento de f por aplicaciones reiteradas. Por ejemplo:

$$1 \to 4 \to 2 \to 1$$

$$3 \to 6 \to 3$$

$$7 \to 10 \to 5 \to 8 \to 4 \to 2 \to 1$$

Probemos que por la aplicación reiterada de esta aplicación se llega siempre a 1 o a 3. Así la proposición $P(n)$ afirmaría que $f^t(n) = 1$ ó 3 para un cierto t. Debemos probar que se cumplen 2. b. i) y 2. b. ii).

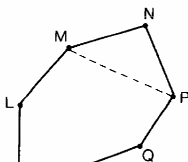
i) $P(1)$ es verdadera dado que $f^3(1) = 1$.

ii) Supongamos $P(k)$ verdadera para todo $k < n$ y probemos que es cierta para n. Si n es par, entonces $f(n) = n/2 < k$; por lo tanto, reiterando f se llega a 1 ó a 3. Sea, pues, $n = 2h + 1$, $h \geq 1$. Se tiene que $f(n) = 2h + 4$ y $f^2(n) = h + 2$. Si $h + 2 < n = 2h + 1$ es posible aplicar la hipótesis inductiva y concluir que la reiteración de f sobre n lleva a 1 ó 3. Queda la posibilidad $h + 2 = 2h + 1$, o sea $h = 1$. En este caso $n = 3$ y sabemos que $f^2(3) = 3$. Hemos probado, entonces, que $P(n)$ es verdadera si $P(k)$ lo es para todo $k < n$. En virtud del principio de inducción concluimos que $P(n)$ es verdadera para todo n.

c) Probar que la suma de los ángulos de un polígono de n lados es $S = 2R(n - 2)$ $(R = 90°)$. Debemos probar que se cumplen 2. c. i) y 2. c. ii).

i) Para $n = 3$ (triángulo $S_3 = 2R(3 - 2) = 2R$), la propiedad es cierta.

ii) Supongamos que es cierta para $n > 3$, $S_n = 2R(n - 2)$ (polígono de n lados), y lo probamos para $n + 1$.



Sea... $LMNPQ$... un polígono de $n + 1$ lados. Si se traza la diagonal MP, se obtienen dos polígonos ...$LMPQ$... y MNP; ...$LMPQ$... tiene n lados: $S_n = 2R(n - 2)$. MNP es triángulo: $S_3 = 2R$. $S_{n+1} = S_n + S_3 = 2R(n - 2) + 2R = 2R[(n + 1) - 2]$, lo que demuestra la validez de la fórmula.

4. Ejemplos y Ejercicios

En lo que sigue se dan algunos ejemplos resueltos, así como también ejercicios, con el objeto de familiarizar al lector con el uso del principio de inducción.

Ejemplo. Hallar el número de subconjuntos de un conjunto finito de n elementos.

Sea X un conjunto finito de n elementos. Sin pérdida de generalidad cabe suponer $X = [1, n]$, el intervalo natural inicial de orden n. Sea $P(n)$ la proposición: "El número total de subconjuntos de X es 2^n". Se probará que $P(n)$ es verdadera para todo $n \in N$.

a) $P(1)$ es verdadera. En efecto, $X = \{1\}$ consta de dos únicos subconjuntos: ϕ y $\{1\}$.

b) Supongamos que $P(n)$ es verdadera: Si $X = [1, n]$ el número de subconjuntos es 2^n. Sea $X = [1, n+1]$. Clasifiquemos los subconjuntos de X en dos clases:

A: = {subconjuntos de X que contienen a $n+1$}, y

B: = {subconjuntos de X que no contienen a $n+1$}

Es claro que B es el conjunto de partes de $[1, n]$ y, por lo tanto, B tiene 2^n elementos (hipótesis inductiva). Además, A se obtiene de B agregando a cada subconjunto en B el elemento $n+1$; por lo tanto, A tiene también 2^n elementos. Finalmente, dado que $A \cap B = \phi$, concluimos que el conjunto de partes de X tiene 2^{n+1} elementos, lo cual establece la validez de $P(n+1)$.

Se sigue del principio de inducción que todo conjunto finito de n elementos posee un total de 2^n subconjuntos.

Ejercicio. Sea $f: N \to N$ definida por

$$f(n): = \begin{cases} n/2, & \text{si } n \text{ es par} \\ 3n+1, & \text{si } n \text{ es de la forma } 4k+1 \\ 3n-1, & \text{si } n \text{ es de la forma } 4k-1 \end{cases}$$

Por ejemplo,

$$3 \to 8 \to 4 \to 2 \to 1$$

$$7 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$$

Probar que la aplicación reiterada de f conduce a 1.

Ejemplo. Probemos que para todo $n \in N$, 54 divide a $2^{2n+1} - 9n^2 + 3n - 2$.

a) Para $n = 1$, se verifica que 54 divide a 0. $P(1)$ es verdadera.

b) Supongamos que $P(n)$ es verdadera y lo probamos para $n+1$. Se tiene:

$$2^{2(n+1)} - 9(n+1)^2 + 3(n+1) - 2 = (2^{2n+1} - 9n^2 + 3n - 2) \cdot 2^2 +$$

$$+ 2^2 \cdot 9 \cdot n^2 - 3 \cdot 2^2 n + 8 - 9(n^2 + 2n + 1) + 3(n+1) - 2 =$$

$$= (\text{mult. } 54) + 9n^2(2^2 - 1) - 3n(2^2 + 6 - 1) + (8 - 9 + 1) =$$

$$= (\text{mult. } 54) + n(n-1) \cdot 27$$

y como 2 divide a $n(n-1) = \text{mult. } 54$.

Luego, $P(n+1)$ es verdadera y, por el principio de inducción, $P(n)$ es verdadera para todo n.

Ejercicios.

a) Probar $\forall n,\ n \in N$:

i) $1 + 2 + 3 + \ldots + n = \dfrac{n \cdot (n+1)}{2}$.

ii) $1 + 3 + 5 + \ldots + (2n - 1) = n^2$.

iii) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n \cdot (n+1) \cdot (n+2)}{6}$.

iv) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\dfrac{n \cdot (n+1)}{2}\right)^2$.

v) $1^4 + 2^4 + 3^4 + \ldots + n^4 = \dfrac{n \cdot (n+1) \cdot (2n+1) \cdot (3n^2 + 3n - 1)}{30}$.

vi) $1 \cdot 2 + 2 \cdot 3 + \ldots + n \cdot (n+1) = \dfrac{n \cdot (n+1) \cdot (n+2)}{3}$.

vii) $0 \cdot 1 + 2 + 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \ldots + (n-1) \cdot n \cdot (n+1) =$

$= \frac{1}{4} \cdot (n^2 + n) \cdot (n^2 + n - 2)$.

viii) $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \frac{1}{3} \cdot n \cdot (4n^2 - 1)$.

b. Probar inductivamente las fórmulas siguientes:

i) Progresión aritmética:

$\forall a, b, \in R, \forall n, n \in N$: $a + (a+b) + (a+2b) + \ldots + (a+nb) = \dfrac{(n+1)(2a+nb)}{2}$.

ii) Progresión geométrica:

$\forall a, q \in R, q \neq 1, \forall n, n \in N$: $a + aq + aq^2 + \ldots + aq^n = a \cdot \dfrac{1 - q^{n+1}}{1 - q}$.

c) Analizar, en la proposición que sigue, qué hipótesis del principio de inducción en su primera forma no se satisface:

$$P(n): \ n^2 > 2n + 1$$

Establecer por inducción para cuáles valores de n la proposición es verdadera.

d) Analizar, en las siguientes proposiciones, qué hipótesis del principio de inducción no se satisfacen:

$$P(n); \ n^2 + n + 41 \text{ es primo;}$$

$$P(n): \ n^2 - n + 41 \text{ es primo;}$$

$$P(n): \ n^2 - 79n + 1601 \text{ es primo;}$$

$$P(n): \ \frac{(n-1)(n+1)}{2} \in N;$$

$$P(n): \ \sqrt{n} \in N.$$

e) Probar que $\forall n, \ n \in N$:

i) $7^{2n} - 48n - 1$ es divisible por 2304.

ii) $7^{2n} + 16n - 1$ es divisible por 64.

iii) $3^{2n+2} - 2^{n+1}$ es divisible por 7.

iv) $10^{6n+2} + 10^{3n+1} + 1$ es divisible por 111.

v) $2^{2n+1} - 9n^2 + 3n - 2$ es divisible por 54.

f) **Sucesión de Fibonacci.** Esta es la sucesión definida recursivamente por $u_1 = 1$, $u_2 = 1$, $u_3 = 2$ y $u_n = u_{n-1} + u_{n-2}$, si $n > 2$. Por ejemplo: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377,...

i) Probar que para todo n natural la *fórmula de Binet:*

$$u_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

ii) Probar que para todo n natural $(u_n, u_{n+1}) = 1$, o sea: términos sucesivos de la sucesión de Fibonacci son coprimos.

iii) Probar que para todo par n, m de números naturales

a) $u_{n+m} = u_{m-1} \cdot u_n + u_m \cdot u_{n+1}$.

b) $u_n | u_{nm}$.

(**Sugerencia.** Hacer inducción en n.)

iv) Sea $m = qn + r$ en N. Probar que $(u_m, u_n) = (u_r, u_n)$.

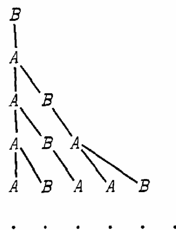
(**Sugerencia.** $(u_m, u_n) = (u_{qn+r}, u_n) = (u_{qn-1}u_r + u_{qn}r_{r+1}, u_n) = (u_{qn-1}u_r, u_n) = (u_r, u_n)$ pues $(u_n, u_{qn-1}) = 1$.)

v) Probar que para todo par n, m de números naturales

$$(u_n, u_m) = u_{(n,m)}.$$

vi) Probar que $u_n | u_m$ si, y sólo si, $n | m$.

Nota Histórica. Leonardo de Pisa, también llamado Fibonacci (contracción de "hijo de Bonacci") es considerado como uno de los matemáticos más destacados de la Edad Media. Su gran obra es el libro "Liber Abaci" (1202 y su revisión de 1228), escrito en el espíritu de la matemática arábiga, donde introduce el sistema de numeración decimal. En este libro aparece un curioso problema conocido con el nombre de "problema de los conejos", *paria coniculorum:* Un hombre posee una pareja de conejos en un recinto cerrado. Si los hábitos de reproducción son que cada pareja procrea una pareja al segundo mes de nacimiento, ¿cuántas parejas pueden engendrarse en un año? Indiquemos con A a la pareja adulta y con B a la pareja bebé. En un diagrama, se tiene:



. . . . . .

Se ve que el diagrama sigue el esquema de la sucesión de Fibonacci. Si el 1 de enero se tiene una pareja adulta, entonces el 31 de diciembre se tendrán 377 parejas.

APENDICE II

TABLA DE PRIMOS MENORES QUE 10.000

2	269	617	1009	1427	1823	2269	2699	3169
3	271	619	1013	1429	1831	2273	2707	3181
5	277	631	1019	1433	1847	2281	2711	3187
7	281	641	1021	1439	1861	2287	2713	3191
11	283	643	1031	1447	1867	2293	2719	3203
13	293	647	1033	1451	1871	2297	2729	3209
17	307	653	1039	1453	1873	2309	2731	3217
19	311	659	1049	1459	1877	2311	2741	3221
23	313	661	1051	1471	1879	2333	2749	3229
29	317	673	1061	1481	1889	2339	2753	3251
31	331	677	1063	1483	1901	2341	2767	3253
37	337	683	1069	1487	1907	2347	2777	3257
41	347	691	1087	1489	1913	2351	2789	3259
43	349	701	1091	1493	1931	2357	2791	3271
47	353	709	1093	1499	1933	2371	2797	3299
53	359	719	1097	1511	1949	2377	2801	3301
59	367	727	1103	1523	1951	2381	2803	3307
61	373	733	1109	1531	1973	2383	2819	3313
67	379	739	1117	1543	1979	2389	2833	3319
71	383	743	1123	1549	1987	2393	2837	3323
73	389	751	1129	1553	1993	2399	2843	3329
79	397	757	1151	1559	1997	2411	2851	3331
83	401	761	1153	1567	1999	2417	2857	3343
89	409	769	1163	1571	2003	2423	2861	3347
97	419	773	1171	1579	2011	2437	2879	3359
101	421	787	1181	1583	2017	2441	2887	3361
103	431	797	1187	1597	2027	2447	2897	3371
107	433	809	1193	1601	2029	2459	2903	3373
109	439	811	1201	1607	2039	2467	2909	3389
113	443	821	1213	1609	2053	2473	2917	3391
127	449	823	1217	1613	2063	2477	2927	3407
131	457	827	1223	1619	2069	2503	2939	3413
137	461	829	1229	1621	2081	2521	2953	3433
139	463	839	1231	1627	2083	2531	2957	3449
149	467	853	1237	1637	2087	2539	2963	3457
151	479	857	1249	1657	2089	2543	2969	3461
157	487	859	1259	1663	2099	2549	2971	3463
163	491	863	1277	1667	2111	2551	2999	3467
167	499	877	1279	1669	2113	2557	3001	3469
173	503	881	1283	1693	2129	2579	3011	3491
179	509	883	1289	1697	2131	2591	3019	3499
181	521	887	1291	1699	2137	2593	3023	3511
191	523	907	1297	1709	2141	2609	3037	3517
193	541	911	1301	1721	2143	2617	3041	3527
197	547	919	1303	1723	2153	2621	3049	3529
199	557	929	1307	1733	2161	2633	3061	3533
211	563	937	1319	1741	2179	2647	3067	3539
223	569	941	1321	1747	2203	2657	3079	3541
227	571	947	1327	1753	2207	2659	3083	3547
229	577	953	1361	1759	2213	2663	3089	3557
233	587	967	1367	1777	2221	2671	3109	3559
239	593	971	1373	1783	2237	2677	3119	3571
241	599	977	1381	1787	2239	2683	3121	3581
251	601	983	1399	1789	2243	2687	3137	3583
257	607	991	1409	1801	2251	2689	3163	3593
263	613	997	1423	1811	2267	2693	3167	3607

Continuación...

3613	4079	4567	5051	5557	6053	6553	7027	7573
3617	4091	4583	5059	5563	6067	6563	7039	7577
3623	4093	4591	5077	5569	6073	6569	7043	7583
3631	4099	4597	5081	5573	6079	6571	7057	7589
3637	4111	4603	5087	5581	6089	6577	7069	7591
3643	4127	4621	5099	5591	6091	6581	7079	7603
3659	4129	4637	5101	5623	6101	6599	7103	7607
3671	4133	4639	5107	5639	6113	6607	7109	7621
3673	4139	4643	5113	5641	6121	6619	7121	7639
3677	4153	4649	5119	5647	6131	6637	7127	7643
3691	4157	4651	5147	5651	6133	6653	7129	7649
3697	4159	4657	5153	5653	6143	6659	7151	7669
3701	4177	4663	5167	5657	6151	6661	7159	7673
3709	4201	4673	5171	5659	6163	6673	7177	7681
3719	4211	4679	5179	5669	6173	6679	7187	7687
3727	4217	4691	5189	5683	6197	6689	7193	7691
3733	4219	4703	5197	5689	6199	6691	7207	7699
3739	4229	4721	5209	5693	6203	6701	7211	7703
3761	4231	4723	5227	5701	6211	6703	7213	7717
3767	4241	4729	5231	5711	6217	6709	7219	7723
3769	4243	4733	5233	5717	6221	6719	7229	7727
3779	4253	4751	5237	5737	6229	6733	7237	7741
3793	4259	4759	5261	5741	6247	6737	7243	7753
3797	4261	4783	5273	5743	6257	6761	7247	7757
3803	4271	4787	5279	5749	6263	6763	7253	7759
3821	4273	4789	5281	5779	6269	6779	7283	7789
3823	4283	4793	5297	5783	6271	6781	7297	7793
3833	4289	4799	5303	5791	6277	6791	7307	7817
3847	4297	4801	5309	5801	6287	6793	7309	7823
3851	4327	4813	5323	5807	6299	6803	7321	7829
3853	4337	4817	5333	5813	6301	6823	7331	7841
3863	4339	4831	5347	5821	6311	6827	7333	7853
3877	4349	4861	5351	5827	6317	6829	7349	7867
3881	4357	4871	5381	5839	6323	6833	7351	7873
3889	4363	4877	5387	5843	6329	6841	7369	7877
3907	4373	4889	5393	5849	6337	6857	7393	7879
3911	4391	4903	5399	5851	6343	6863	7411	7883
3917	4397	4909	5407	5857	6353	6869	7417	7901
3919	4409	4919	5413	5861	6359	6871	7433	7907
3923	4421	4931	5417	5867	6361	6883	7451	7919
3929	4423	4933	5419	5869	6367	6899	7457	7927
3931	4441	4937	5431	5879	6373	6907	7459	7933
3943	4447	4943	5437	5881	6379	6911	7477	7937
3947	4451	4951	5441	5897	6389	6917	7481	7949
3967	4457	4957	5443	5903	6397	6947	7487	7951
3989	4463	4967	5449	5923	6421	6949	7489	7963
4001	4481	4969	5471	5927	6427	6959	7499	7993
4003	4483	4973	5477	5939	6449	6961	7507	8009
4007	4493	4987	5479	5953	6451	6967	7517	8011
4013	4507	4993	5483	5981	6469	6971	7523	8017
4019	4513	4999	5501	5987	6473	6977	7529	8039
4021	4517	5003	5503	6007	6481	6983	7537	8053
4027	4519	5009	5507	6011	6491	6991	7541	8039
4049	4523	5011	5519	6029	6521	6997	7547	8053
4051	4547	5021	5521	6037	6529	7001	7549	8059
4057	4549	5023	5527	6043	6547	7013	7559	8069
4073	4561	5039	5531	6047	6551	7019	7561	8081

Continuación...

8087	8291	8537	8731	8941	9161	9377	9587	9791
8089	8293	8539	8737	8951	9173	9391	9601	9803
8093	8297	8543	8741	8963	9181	9397	9613	9811
8101	8311	8563	8747	8969	9187	9403	9619	9817
8111	8317	8573	8753	8971	9199	9413	9623	9829
8117	8329	8581	8761	8999	9203	9419	9629	9833
8123	8353	8597	8779	9001	9209	9421	9631	9839
8147	8363	8599	8783	9007	9221	9431	9643	9851
8161	8369	8609	8803	9011	9227	9433	9649	9857
8167	8377	8623	8807	9013	9239	9437	9661	9859
8171	8387	8627	8819	9029	9241	9439	9677	9871
8179	8389	8629	8821	9041	9257	9461	9679	9883
8191	8419	8641	8831	9043	9277	9463	9689	9887
8209	8423	8647	8837	9049	9281	9467	9697	9901
8219	8429	8663	8839	9059	9283	9473	9719	9907
8221	8431	8669	8849	9067	9293	9479	9721	9923
8231	8443	8677	8861	9091	9311	9491	9733	9929
8233	8447	8681	8863	9103	9319	9497	9739	9931
8237	8461	8689	8867	9109	9323	9511	9743	9941
8243	8467	8693	8887	9127	9337	9521	9749	9949
8263	8501	8699	8893	9133	9341	9533	9767	9967
8269	8513	8707	8923	9137	9343	9539	9769	9973
8273	8521	8713	8929	9151	9349	9547	9781	
8287	8527	8719	8933	9157	9371	9551	9787	

BIBLIOGRAFIA

I. Textos Elementales

EYNDEN, CH. V. Number Theory, An Introduction to Proof, International Textboox Co., Filadelfia, Penn. (1970).

LEVEQUE, W.J. Elementary Theory of Numbers, Addison-Wesley, Reading, Mass. (1962).

NIVEN, I. y ZUCKERMAN, H. An Introduction to the Theory of Numbers, Wiley, Nueva York, N.Y. (1972).

RADEMACHER, H. Lectures on Elementary Number Theory, Blaisdell, Nueva York, N.Y. (1964).

SHOCKLEY, J.E. Introduction to Number Theory, Holt, Rinehart & Winston, Inc., Nueva York, N.Y. (1967).

STARK, H. An Introduction to Number Theory, Markham, Chicago, Ill. (1970).

USPENSKY, J. y HEASLET, M.A. Elementary Number Theory, McGraw, Nueva York, N.Y. (1939).

VINOGRADOV, I. Fundamentos de la Teoría de Números, Editorial Mir, Moscú (1971).

II. Textos más Avanzados

HARDY, G.H. y WRIGHT, E.M. An Introduction to the Theory of Numbers, Oxford Univ. Press, Londres, 4a. edición (1962).

HASSE, H. Vorlesungen über Zahlentheorie, Springer-Verlag, Berlín (1964).

LANDAU, E. Elementary Number Theory, Chelsea Publishing Co., Nueva York, N.Y. (1952). (Traducción del alemán de "Aus der Elementaren Zahlentheorie", 1927.)

LEVEQUE, W.J. Topics in Number Theory, Addison-Wesley, Reading, Mass., 2 vols. (1956).

III. Referencias de Tipo Histórico

DICKSON, L. History of the Theory of Numbers, Chelsea Publishing Co., Nueva York, N.Y., 3 vols. (1952).

Mathematical Monthly. Una excelente revista que presenta artículos de divulgación es *Scientific American*. En ella se publican los famosos artículos de Martín Gardner.

COLECCION DE MONOGRAFIAS CIENTIFICAS

Publicadas

Serie de matemática

Nº 1. La Revolución en las Matemáticas Escolares, por el Consejo Nacional de Maestros de Matemáticas de los Estados Unidos de América.
Nº 2. Espacios Vectoriales y Geometría Analítica, por Luis A. Santaló.
Nº 3. Estructuras Algebraicas I, por Enzo R. Gentile.
Nº 4. Historia de las Ideas Modernas en la Matemática, por José Babini.
Nº 5. Algebra Lineal, por Orlando E. Villamayor.
Nº 6. Algebra Linear e Geometria Euclideana, por Alexandre Augusto Martins Rodrigues.
Nº 7. El Concepto de Número, por César A. Trejo.
Nº 8. Funciones de Variable Compleja, por José I. Nieto.
Nº 9. Introducción a la Topología General, por Juan Horváth.
Nº 10. Funções Reais, por Djairo G. de Figueiredo.
Nº 11. Probabilidad e Inferencia Estadística, por Luis A. Santaló.
Nº 12. Estructuras Algebraicas II (Algebra Lineal), por Enzo R. Gentile.
Nº 13. La Revolución en las Matemáticas Escolares (Segunda Fase), por Howard F. Fehr, John Camp y Howard Kellog.
Nº 14. Estructuras Algebraicas III (Grupos Finitos), por Horacio H, O'Brien.
Nº 15. Introducción a la Teoría de Grafos, por Fausto A. Toranzos.
Nº 16. Estructuras Algebraicas IV (Algebra Multilineal), por Artibano Micali y Orlando E. Villamayor.
Nº 17. Introdução à Análise Funcional: Espaços de Banach e Cálculo Diferencial, por Leopoldo Nachbin.
Nº 18. Introducción a la Integral de Lebesgue en la Recta, por Juan Antonio Gatica.
Nº 19. Introducción a los Espacios de Hilbert, por José I. Nieto.
Nº 20. Elementos de Biomatemática, por Alejandro B. Engel.
Nº 21. Introducción a la Computación, por Jaime Michelow.
Nº 22. Estructuras Algebraicas V (Teoría de Cuerpos), por Héctor A. Merklen.
Nº 23. Estructuras Algebraicas VI (Formas Cuadráticas), por Francisco M. Piscoya.
Nº 24. Estructuras Algebraicas VII (Estructuras de Algebras), por Artibano Micali.
Nº 25. Aritmética Elemental, por Enzo R. Gentile.

Serie de física

Nº 1. Concepto Moderno del Núcleo, por D. Allan Bromley.
Nº 2. Panorama de la Astronomía Moderna, por Félix Cernuschi y Sayd Codina.
Nº 3. La Estructura Electrónica de los Sólidos, por Leopoldo M. Falicov.

N° 4. Física de Partículas, por Igor Saavedra.
N° 5. Experimento, Razonamiento y Creación en Física, por Félix Cernuschi.
N° 6. Semiconductores, por George Bemski.
N° 7. Aceleradores de Partículas, por Fernando Alba Andrade.
N° 8. Física Cuántica, por Onofre Rojo y Harold V. McIntosh.
N° 9. La Radiación Cósmica, por Gastón R. Mejía y Carlos Aguirre.
N° 10. Astrofísica, por Carlos Jaschek y Mercedes C. de Jaschek.
N° 11. Ondas, por Oscar J. Bressan y Enrique Gaviola.
N° 12. El Láser, por Mario Garavaglia.
N° 13. Teoría Estadística de la Materia, por Antonio E. Rodríguez y Roberto E. Caligaris.
N° 14. Aplicações da Teoria de Grupos na Espectroscopia Raman e do Infra-Vermelho, por Jorge Humberto Nicola y Anildo Bristoti.

Serie de química

N° 1. Cinética Química Elemental, por Harold Behrens Le Bas.
N° 2. Bioenergética, por Isaias Raw y Walter Colli.
N° 3. Macromoléculas, por Alejandro Paladini y Moisés Burachik.
N° 4. Mecanismo de las Reacciones Orgánicas, por Jorge A. Brieux.
N° 5. Elementos Encadenados, por Jacobo Gómez Lara.
N° 6. Enseñanza de la Química Experimental, por Francisco Giral.
N° 7. Fotoquímica de Gases, por Ralf-Dieter Penzhorn.
N° 8. Introducción a la Geoquímica, por Félix González-Bonorino.
N° 9. Resonancia Magnética Nuclear de Hidrógeno-1 y de Carbono-13, por Pedro Joseph-Nathan.
N° 10. Cromatografía Líquida de Alta Presión, por Harold M. McNair y Benjamín Esquivel H.
N° 11. Actividad Optica, Dispersión Rotatoria Optica y Dicroísmo Circular en Química Orgánica, por Pierre Crabbé.
N° 12. Espectroscopia Infrarroja, por Jesús Morcillo Rubio.
N° 13. Polarografía, por Alejandro J. Arvía y Jorge A. Bolzán.
N° 14. Paramagnetismo Electrónico, por Juan A. McMillan.
N° 15. Introducción a la Estereoquímica, por Juan A. Garbarino.
N° 16. Cromatografía en Papel y en Capa Delgada, por Xorge A. Domínguez.
N° 17. Introducción a la Espectrometría de Masa de Sustancias Orgánicas, por Otto R. Gottlieb y Raimundo Braz Filho.
N° 18. Cinética Química, por Rodolfo V. Caneda.
N° 19. Fuerzas Intermoleculares, por Mateo Díaz Peña.
N° 20. Físico-Química de Superficies, por Tibor Rabockai.
N° 21. Corrosión, por José R. Galvele.
N° 22. Introducción a la Electroquímica, por Dionisio Posadas.
N° 23. Cromatografía de Gases, por Harold M. McNair.
N° 24. Cinética de Disolución de Medicamentos, por Edison Cid Cárcamo.
N° 25. Introducción a la Química de Suelos, por Elemer Bornemisza.
N° 26. Elementos de Catálisis Heterogénea, por Sergio E. Droguett.
N° 27. Introducción a la Electrocatálisis, por Alejandro J. Arvía y María Cristina Giordano.
N° 28. Química de Sólidos, por Julio César Bazán.

N° 29. Química Bioinorgânica, por Henrique Eisi Toma.
N° 30. Introducción al Estudio de los Productos Naturales, por Eduardo G. Gros, Alicia B. Pomilio, Alicia M. Seldes y Gerardo Burton.

Serie de biología

N° 1. La Genética y la Revolución en las Ciencias Biológicas, por José Luis Reissig.
N° 2. Bases Ecológicas para la Explotación Agropecuaria en la América Latina, por Guillermo Mann F.
N° 3. La Taxonomía y la Revolución en las Ciencias Biológicas, por Elías R. de la Sota.
N° 4. Principios Básicos para la Enseñanza de la Biología, por Oswaldo Frota-Pessoa.
N° 5. A Vida da Célula, por Renato Basile.
N° 6. Microorganismos, por J. M. Gutiérrez-Vázquez.
N° 7. Principios Generales de Microbiología, por Norberto J. Palleroni.
N° 8. Los Virus, por Enriqueta Pizarro-Suárez y Gamba.
N° 9. Introducción a la Ecología del Bentos Marino, por Manuel Vegas Vélez.
N° 10. Biosíntesis de Proteínas y el Código Genético, por Jorge E. Allende.
N° 11. Fundamentos de Inmunología e Inmunoquímica, por Félix Córdoba Alva y Sergio Estrada Parra.
N° 12. Bacteriófagos, por Romilio Espejo T.
N° 13. Biogeografía de América Latina, por Angel L. Cabrera y Abraham Willink.
N° 14. Relación Hospedante-Parásito. Mecanismo de Patogenicidad de los Microorganismos, por Manuel Rodríguez Leiva.
N° 15. Genética de Poblaciones Humanas, por Francisco Rothhammer.
N° 16. Introducción a la Ecofisiología Vegetal, por Ernesto Medina.
N° 17. Aspectos de Biología Celular y la Transformación Maligna, por Manuel Rieber.
N° 18. Transporte a Través de la Membrana Celular, por P. J. Garrahan y A. F. Rega.
N° 19. Duplicación Cromosómica y Heterocromatina a Nivel Molecular y Citológico, por Nestor O. Bianchi.
N° 20. Citogenética Básica y Biología de los Cromosomas, por Francisco A. Sáez y Horacio Cardoso.
N° 21. Ecología de Poblaciones Animales, por Jorge E. Rabinovich.
N° 22. Metodología para el Estudio de la Vegetación, por Silvia D. Matteucci y Aída Colma.
N° 23. Los Sistemas Ecológicos y la Humanidad, por Ariel E. Lugo y Gregory L. Morris.
N° 24. A Germinação das Sementes, por Luiz Gouvêa Laboriau.
N° 25. Introducción a la Farmacocinética, por Edison Cid Cárcamo.
N° 26. Introducción a la Teoría y Práctica de la Taxonomía Numérica, por Jorge Víctor Crisci y María Fernanda López Armengol.
N° 27. ¿Qué es la Diferenciación Celular?, por Roberto B. García y Susana Pereyra Alfonso.
N° 28. Limnología Sanitaria, Estudio de la Polución de Aguas Continentales, por Samuel Murgel Branco.

N° 29. Etología: El Estudio Biológico del Comportamiento Animal, por Raúl Vaz-Ferreira.
N° 30. Fotosíntesis, por Carlos S. Andreo y Rubén H. Vallejos.

En preparación

Serie de matemática

Geometrías Finitas, por Oscar Barriga.
Algebra Elemental, por Leopoldo Nachbin.
Computadoras y Procesamiento de Datos, por Julio Villanueva y Oscar Harasic.
Principios Matemáticos da Dinâmica dos Fluidos, por Guilherme M. de la Penha.
Análisis Multivariado-Método de Componentes Principales, por Laura Pla.

Serie de física

Teoría de Fluidos en Equilibrio, por Antonio E. Rodríguez y Roberto E. Caligaris.
Fundamentos de Cristalografía Física, por Jaime Rodríguez Lara.

Serie de química

Fisicoquímica de Interfases, por Francisco Javier Garfias.

Serie de biología

Cromosomas Humanos y de Primates, por Máximo E. Drets y Héctor Seuanez.
La Pesca y la Piscicultura en Aguas Continentales de América Latina, por Argentino A. Bonetto y Hugo P. Castello.
Fitomorfología Funcional y Adaptativa, por Elías R. de la Sota.
Fundamentos de Genética Biométrica y sus Aplicaciones al Mejoramiento Genético, por Jorge A. Mariotti.
Origen y Anatomía del Cromosoma Eucarionte, por Nestor O. Bianchi.
Limnología Básica, por José Galizia Tundisi.

Nota. Las personas interesadas en adquirir estas monografías deben dirigirse a la Oficina de Ventas y Promoción, Departamento de Información Pública, Organización de los Estados Americanos, Washington, D. C., 20006-4499 o a las Oficinas de la OEA en el país respectivo.